jamk.fi

SDN:n tutkimustilanteen nykytilan kartoitus kyberturvallisuuden viitekehyksessä

Olli Honkasalo

Opinnäytetyö
Joulukuu 2014

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Honkasalo, Olli	Opinnäytetyö	11.12.2014
	Sivumäärä 51 + 5	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: kyllä

Työn nimi

SDN:n tutkimustilanteen nykytilan kartoitus kyberturvallisuuden viitekehyksessä

Koulutusohjelma

Tietotekniikan koulutusohjelma

Työn ohjaaja(t)

Piispanen Juha, Saharinen Karo

Toimeksiantaja(t)

Jyvsectec, Jari Hautamäki

Tiivistelmä

Työssä oli tarkoituksena tutustua SDN-verkkojen nykytilaan, tämänhetkisiin laitteisiin, protokolliin sekä ratkaisuihin, kuten myös löytää esimerkkejä sitä käyttävistä yrityksistä. Erityishuomiona piti tarkastella sen vaikutusta tietoturvaan.

Lähteinä työssä käytettiin pääasiassa alan sivustoja, asiantuntijoiden blogeja, valmistajien ja projektien verkkosivuja, sekä hieman myös kirjallisuutta, jota aiheen tuoreuden takia oli heikosti löydettävissä.

Työn aikana kävi ilmi, että SDN on saanut voimakkaasti huomiota markkinointiterminä, mutta mitään selkeää yksittäistä merkitystä termillä ei enää ole, jos on koskaan ollutkaan. Protokollia on käytössä laidasta laitaan aina alkuperäisestä SDN-protokollana tunnetusta OpenFlowsta uudempiin tekijöihin kuten OpFlex sekä vanhempiin SDN-termillä markkinoitaviin kuten BGP ja XMPP.

SDN voi tuoda huomattavia säästöjä poistamalla paljon manuaalista toistuvaa työtä verkon hallinnasta. Automatisoimalla laitteiden konfiguroinnin se omalta osaltaan auttaa myös ehkäisemään inhimillisiä virheitä ja sitä kautta parantaa myös tietoturvaa. Toisaalta SDN-kontrolleri muodostaa selvän yksittäisen pisteen johon kohdistettu onnistunut hyökkäys voi lamauttaa tehokkaasti koko verkon.

Tutkimusta tällä hetkellä ajetaan eteenpäin niin avoimissa projekteissa kuin verkkojättien suljettujen ovien takana, eikä oikeastaan kukaan tiedä mikä tai kuka tulee lähivuosina luomaan sen sovelluksen, joka tuo SDN:n jokaiseen isompaan datakeskukseen.

Avainsanat (asiasanat)

SDN, OpenFlow, Tietoverkot

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Description

Author(s)	Type of publication	Date
Honkasalo, Olli	Bachelor's thesis	11.12.2014
		Language of publication: Finnish
	Number of pages 51 + 5	Permission for web publication: yes

Title of publication

SDN - Current state of research within cybersecurity framework

Degree programme

Information Technology

Tutor(s)

Piispanen Juha, Saharinen Karo

Assigned by

Jyvsectec, Jari Hautamäki

Abstract

The purpose of the thesis was to look into the current state of SDN, devices, protocols, solutions and to find examples of real life implementations. Special attention was to be paid to how its effects on network security.

Sources used were mostly industry web sites, expert blogs, manufacturer and project web pages and some literature, which unfortunately was slim, caused by the novelty of the subject.

During the research it became quickly apparent that SDN had gained a strong interest as a marketing term and had lost almost all specific meaning, if it ever had any. Protocols in use go from the original SDN protocol, OpenFlow, to newer ones such as OpFlex to much older ones like BGP and XMPP.

SDN can bring cost saving by eliminating much of the manual repeated labor in network management. By automating the network configuration it also helps to prevent human errors and through that helps to improve security. Although SDN controller creates a single point of weakness which - when successfully attacked - can effectively shut down the whole network.

The research of SDN is currently driven forwards in both open projects and behind closed doors of network giants. At this time it is impossible for anyone to say what or who will create the "killer app" that will bring SDN to every larger datacenter.

Keywords/tags (subjects)

SDN, OpenFlow, Networks

Miscellaneous

Sisällysluettelo

Kuviot

Lyhenteet

AAA – Authentication, Authorization and Accounting; Todentaminen, valtuutus ja tilastointi. Menetelmä, jolla voidaan tunnistaa toinen osapuoli tietoverkossa.

ACI – Application Centric Infrastructure; Ohjelmistokeskeinen Infrastruktuuri.

ACL – Access Control List; Työkalu käyttöoikeuksien ja niiden periytyvyyden hallintaan.

AMQ – Automated Malware Quarantine; Tekniikka automaattiseen haittaohjelmien eristämiseen.

API – Application Programming Interface; Ohjelmointirajapinta. Määritelmä, jonka mukaan eri ohjelmat voivat tehdä pyyntöjä ja vaihtaa tietoja eli keskustella keskenään.

ASIC – Application Specific Integrated Circuit; Sovelluskohtainen mikropiiri. Mikropiiri, joka on suunniteltu tietyn sovelluksen tarpeisiin.

BGP – Border Gateway Protocol; Internetin reititysprotokolla autonomisten järjestelmien välille.

HAL – Hardware Abstraction Layer; Fyysisen OpenFlow-yhteensopivan kytkimen abstraktointitaso.

LTS – Long-Term Support; Ohjelmiston versio jolle luvataan tuki ja päivitykset pisimmälle aikavälille. Saa usein päivityksiä vuosien ajan tulevaisuuteen.

NETCONF - Network Configuration Protocol; Verkonhallintaprotokolla joka luotiin vuonna 2006 tukemaan SNMP:tä. Mahdollistaa konfiguraatioiden lähettämisen, muokkaamisen ja poistamisen etänä verkkolaitteilta.

NFV – Network Functions Virtualization; Verkkofunktioiden virtualisointi. Tekniikka jossa verkon perinteisesti fyysisten komponenttien toimintoja, kuten palomuuri tai kuormantasaus, annetaan yhden tai useamman virtuaalikoneen hoidettavaksi.

ONF – Open Networking Foundation; Voittoa tavoittelematon organisaatio SDN:n ja OpenFlown kehittämiseksi.

REST – Representational state transfer; HTTP-protokollaan perustuva arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen.

SDN – Software-Defined Networking; Koko tämän työn aihe.

SNMP – Simple Network Management Protocol; TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla. Luotiin vuonna 1988 verkkojen hallintaan, mutta käytetään pääasiassa tiedustelemaan verkossa olevan laitteen tilaa tai laitteen toimesta antamaan hälytyksiä.

SSL – Secure Socket Layer; Käytöstä poistuva salausprotokolla. Nykyään SSL on korvattu TLS:llä.

TLS – Transport Layer Security; Varmenteisiin perustuva salausprotokolla. SSL:n seuraaja. Käytetään TCP/IP-verkossa suojaamaan kahden pisteen välillä tapahtuva liikenne. Toimii TCP/IP-mallin sovelluskerroksella.

TOR – Top-of-Rack; Kirjaimellisesti kaapin tai ”räkin” päällä oleva kytkin, joka yhdistää kaapissa olevat laitteet verkkoon.

VM – Virtual Machine; Virtuaalikone. Ohjelmallisesti toteutettu tietokone, jossa voidaan ajaa ohjelmia kuin aidossa koneessa.

1 Toimeksiantaja ja tavoite

Toimeksiantajana toimii Jyväskylän ammattikorkeakoulun IT-instituuttiin kuuluva Jyvsectec-projekti, joka tulee sanoista Jyväskylä Security Technology. Jyvsectec ylläpitää ja kehittää kyberturvallisuuden kehitysympäristöä (RGCE, Realistic Global Cyber Environment), jossa tuotetaan palveluita yhteistyöverkoston käyttöön. (JYVSECTEC 2014.)

Jyväskylän ammattikorkeakoulu on kansainvälinen korkeakoulu, jonka yksiköitä ovat ammatillinen opettajakorkeakoulu, hyvinvointiyksikkö, liiketoimintayksikkö sekä teknologiayksikkö. Toimipisteitä on eri puolilla Jyväskylää sekä Saarijärven Tarvaalassa. JAMKissa on yhteensä 8500 opiskelijaa. Vuosittain tietotekniikan insinööri- ja tradenomiopiskelijoiksi otetaan lähemmäs kaksi sataa uutta opiskelijaa. (Tutustu JAMKiin 2014.)

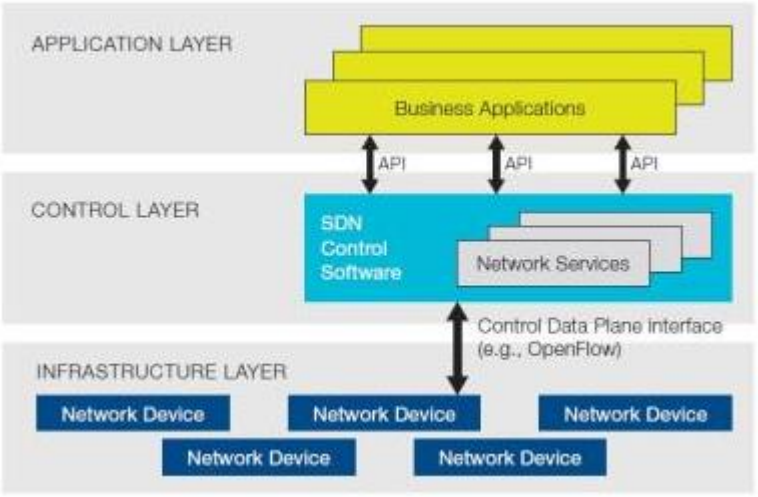
Tavoitteena oli tutustua SDN-verkkojen nykytilaan, mukaan lukien tämänhetkiset laitteet, protokollat ja valmiit ratkaisut. Työssä havaittiin miten nykytilanteeseen on päästy ja mihin tästä ollaan menossa. Erityishuomiona katsastetaan tietoturvan tila ja verrattiin siltä osin perinteisempiin verkkoratkaisuihin.

2 SDN

2.1 Mikä on SDN?

Software-Defined Networking, eli ohjelmallisesti määritelty verkko on nouseva verkkoarkkitehtuuri, jossa verkon hallinta on erotettu pakettien välityksestä ja on suoraan ohjelmoitavissa. Aiemmin tiukasti verkkolaitteisin sidottu hallinta ulkoistetaan helpommin lähestyttävään kontrolleriin. Samalla mahdollistetaan sovelluksille ja verkkopalveluille koko infrastruktuurin käsittely yhtenä loogisena kokonaisuutena. (Brant 2013.)

Loogisesti katsottuna SDN-verkko koostuu kolmesta tasosta: Sovellus (eng: application), hallinta (eng: control) ja infrastruktuuri (eng: infrastructure). Tämä on visualisoitu kuviossa 1.



Kuvio 1. Looginen SDN-verkko (Brant 2013)

Verkon älykkyys on keskitetty ohjelmistopohjaisille SDN-kontrollereille, jotka ylläpitävät kuvaa koko verkosta. Tämän tuloksena koko verkko saadaan näkymään sovelluksille ja käytäntöjen luojille yhtenä loogisena kytkimenä. SDN:n avulla yritykset ja palveluntarjoajat saavat laitevalmistajariippumattoman hallinnan koko verkkoon yhdestä loogisesta pisteestä, virtaviivaistaen verkon suunnittelua ja operointia. SDN

myös yksinkertaistaa verkon laitteita huomattavasti, sillä niiden ei tarvitse enää ymmärtää ja prosessoida tuhansia eri protokollien käskyjä, vaan ainoastaan ottaa vastaan protokollan mukaiset käskyt SDN-kontrollereilta. (Mt.)

Ehkäpä tärkeimpänä seikkana verkon ylläpitäjät voivat ohjelmallisesti hallinnoida koko yksinkertaistettua kokonaisuutta ilman, että heidän täytyy kirjoittaa käsin kymmeniä tuhansia rivejä tuhansille eri laitteille. Lisäksi hyödyntämällä SDN-kontrollerin keskitettyä älyä voidaan verkon käyttäytymistä muokata reaaliajassa ja ottaa käyttöön uusia verkkosovelluksia ja palveluita jopa tunneissa tai päivissä, kun se aiemmin saattoi viedä viikkoja tai kuukausia. (Mt.)

Keskittämällä verkon tilan ohjauskerrokselle SDN antaa verkon ylläpitäjille joustavuuden konfiguroida, hallita, suojata ja optimoida verkon resursseja dynaamisen automatisoidun SDN-kontrollerisovelluksen avulla. Sen lisäksi uusia ominaisuuksia voidaan lisätä suoraan ohjelmaan ilman, että täytyisi odottaa laitevalmistajan lisäävän niitä heidän omiin suljettuihin laitejärjestelmiin. (Mt.)

Nykyinen OpenFlow-protokollaan perustuva SDN-arkkitehtuuri sisältää ohjelmointirajapintoja, joihin voi implementoida yleisiä verkkopalveluita, kuten reititys, multicast, tietoturva, käyttöoikeuksien valvonta, kaistanjako, liikenteen suunnittelu, liikenteen priorisointi (QoS), suorittimen ja tallennuksen optimointi, virran hallinta sekä käytäntöjen hallinnat. SDN-arkkitehtuurin kautta tehtyjä käytäntöjä on helppo määrittää ja ylläpitää niin langallisissa kuin langattomissa verkoissa. (Mt.)

2.2 Tarve

Vuonna 2013 tehdyn tutkimuksen mukaan 91 % vastanneista tietoverkkopäättäjistä koki, että nykyiset tietoverkkojen infrastruktuurit tarvitsevat vielä merkittäviä parannuksia, jotta ne vastaavat jatkuvasti muuttuvien virtualisoinnin ja pilvipalveluiden tarpeita. (Brocade 2013.) Tämän lisäksi nykyinen valtava määrä eri laitteita ja protokollia aiheuttaa sen, että uusien ideoiden kokeileminen varsinkin todellisuutta vastaavilla kuormilla on jatkuvasti vaikeampaa. (OpenFlow Enabling Innovation 2008.)

Laitteiden hallinta oli myös monesti työlästä. Päästäksesi muokkaamaan yhtä asetusta, joutui yhteyden ottamisen jälkeen kulkemaan haluttuun osaan usean peräkkäisen eri komennon kautta. Yleiskäyttöisten skriptien kirjoittaminen ei myöskään ollut mahdollista, sillä eri valmistajien verkkolaitteet ovat käyttäneet perinteisesti eri käyttöjärjestelmiä, ja käyttöliittymä voi vaihdella paljon jopa saman valmistajan laitteiden ja ohjelmistoversioiden välillä. (Dutt 2013.)

Perinteiset tekniikat aiheuttavat myös rajoituksia verkon toiminnalle moderneissa virtualisoiduissa datakeskuksissa. Monimutkaisen ja hitaan hallinnan lisäksi vastaan voi tulla aivan oikeita rajoja, kuten 4096 VLAN:in maksimi. Resursseja täytyy myös varata korkeimman tarpeen mukaan, mikä voi johtaa niiden hukkaan heittämiseen. (VMware NSX 2013.)

2.3 Hyödyt

Paul Brant nimesi neljä SDN:n avainosaa seuraavasti

1. Kehysten ja pakettien ohjaamisen hallinta sekä käytäntöjen määrittäminen
2. Edellisen tekeminen skaalautuen samalla dynaamisesti tarpeen mukaan
3. Mahdollisuus tulla ohjelmoiduksi
4. Läpinäkyvyyden ja hallittavuuden tuominen keskitetyn hallinnan kautta (Brant 2013).

Hänen mukaansa SDN:n ensisijainen tarkoitus ei ole verkon virtualisoiminen. Siinä on kyse verkkojen suunnittelusta, rakentamisesta ja hallinnasta niin, että verkko vastaisi joustavuudeltaan yrityksen tarpeisiin. Tarkoituksena on mahdollistaa sovellusten tuominen ulos tunneissa, ei viikoissa, sekä potentiaalisesti vähentää verkon päivityksen kustannuksia edullisempien yksinkertaisempien laitteiden muodossa. (Mt.)

SDN mahdollistaa verkon koko kuvan muodostamisen, huomioiden sekä fyysiset että virtuaaliset osat. Molempien puolien hallinta onnistuu myös samoilla rajapinnoilla. Verkon tietoturva myös paranee fyysisten ja virtuaalisten laitteiden tietoturvan ja käytäntöjen keskitetyllä hallinnalla. SDN-järjestelmä kykenee myös kokonaisvaltaisen kuvan ansiosta paremmin priorisoimaan liikennettä. (Big Data Blog 2014.)

Edullisemmat yksinkertaisemmat laitteet voivat pienentää hankintakustannuksia, kun taas keskittämisen ja automatisoinnin tuomat edut niin virheiden vähenemisenä kuin toimintojen nopeutumisena tuovat myös yhtiölle säästöjä pidemmällä aikavälillä. Valitettavasti tarkkoja lukuja säästöjen määrästä ei toistaiseksi ollut saatavilla. (Mt.)

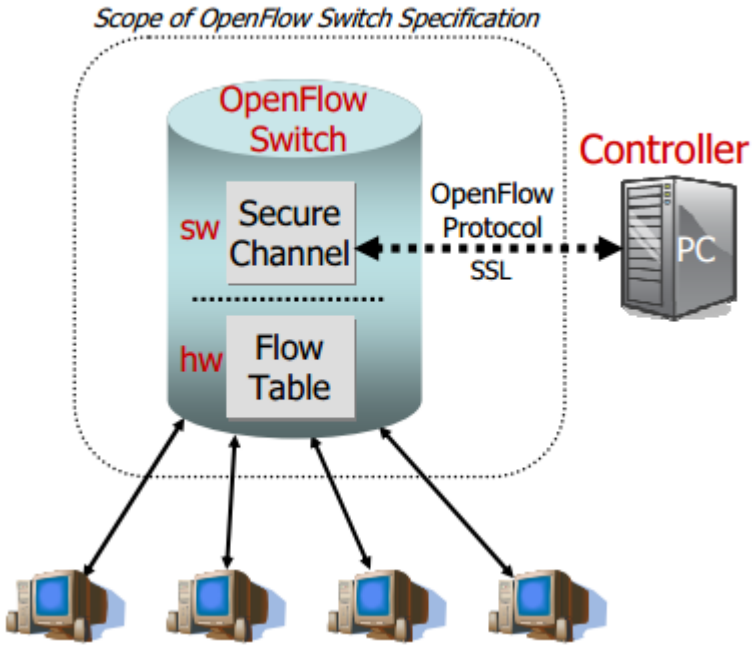
2.4 SDN protokollat

2.4.1 OpenFlow

OpenFlow sai alkunsa Stanfordin ja Berkeleyn yliopistojen tutkijoiden yhteistyössä tarkoituksena tarjota ensimmäinen standardoitu liittymä kontrolli- ja ohjaustasojen välille. Vuoden 2011 maaliskuussa SDN:n ja OpenFlown edistämiseksi perustettiin lukuisten merkittävien verkkoyhtiöiden yhteistyössä Open Networking Foundation (ONF). Perustajia olivat Google, Yahoo, Microsoft, Facebook sekä Euroopan suurin teleoperaattori Deutsche Telekom sekä yhdysvaltalainen teleoperaattori Verizon. (HP OpenFlow Firmware 2011.)

OpenFlow on protokolla, jota käytetään SDN-verkoissa tuomaan kontrollerilla määritellyt komennot OpenFlowta tukeville verkkolaitteille. OpenFlow oli ensimmäinen nimenomaan SDN-verkoille suunniteltu protokolla, ja se mahdollistaa aiempaa syvemmän pääsyn verkkolaitteiden käskyihin, minkä puute oli ollut rajoittavana tekijänä ensimmäisille SDN-tekniikoille vuosituhannen ensi vuosina. (Mt.)

Kuten kuviosta 2 nähdään, OpenFlow-kytkin koostuu vähintään kolmesta osasta: Vuotaulusta (eng: flow table), jossa jokaiseen vuomerkintään yhdistetään toiminto, joka kertoo kytkimelle, miten kyseinen vuo tulisi käsitellä. Suojatusta kanavasta, joka yhdistää kytkimen ulkoiseen hallintaprosessiin (kutsumanimeltään kontrolleriin) mahdollistaen komentojen ja pakettien välittämisen kytkimen ja kontrollerin välillä. Sekä OpenFlow-protokollasta, joka tarjoaa avoimen ja standardoidun tavan kontrollerille viestiä kytkimen kanssa. (Mt.)



Kuvio 2. OpenFlow-kytkin (Sowell 2013)

Jokaiselle vuomerkinnälle on yhdistettynä toiminto. Kolme yksinkertaista perusmerkintää, joita kaikkien OpenFlow-kytkinten tulee tukea, ovat

1. Välittää kyseisen vuon paketit annettuun porttiin tai portteihin mahdollistaen pakettien reitityksen verkon läpi.

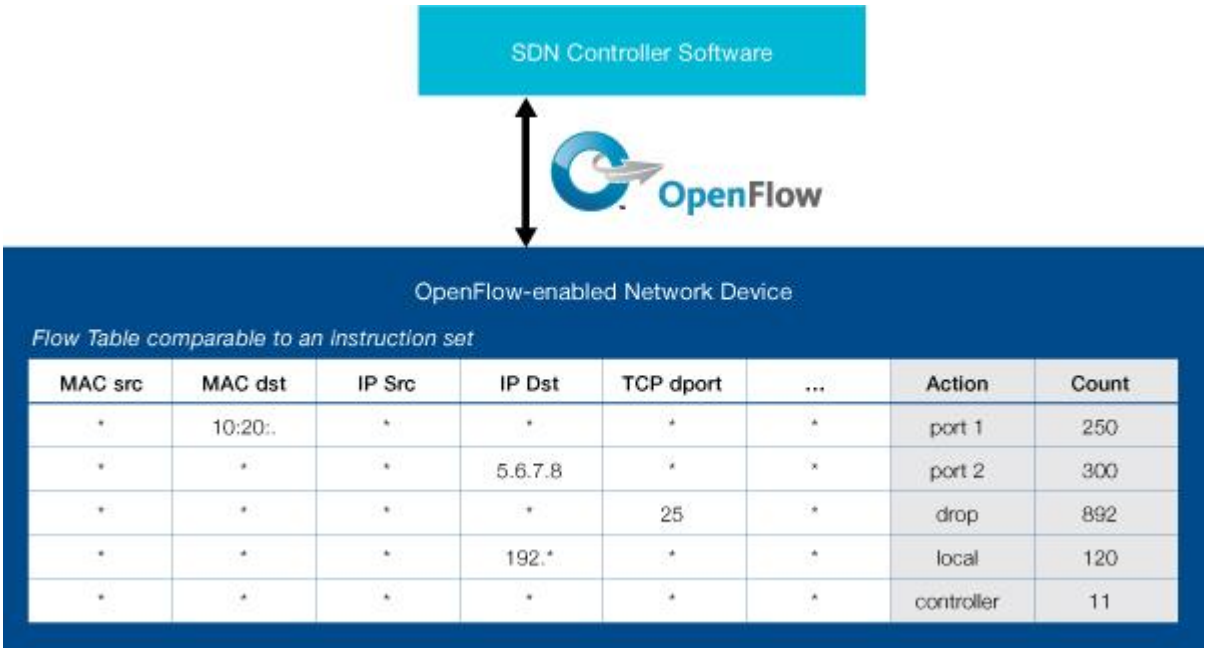
2. Kapseloida ja välittää vuon paketit kontrollerille. Paketti toimitetaan suojatulle kanavalle, jossa se kapseloidaan ja lähetetään kontrollerille. Yleensä tehdään vuon ensimmäiselle paketille, jotta kontrolleri voi päättää, pitäisikö vuo lisätä vuotauluun, tai joissain tapauksissa ohjata kaikki vuon paketit kontrollerille käsiteltäviksi.

3. Pudottaa yksittäisen vuon paketit. Voidaan käyttää tietoturvatarkoituksessa, rajoittaa palveluestohyökkäyksiä tai vähentää turhaa broadcast-selvitysliikennettä. (Mt.)

OpenFlowlla toteutettu SDN mahdollistaa uusien tekniikoiden kokeilun entistä helpommin esimerkiksi rajaamalla osia verkosta uusien kokeilujen piiriin. Verkon ylläpitäjä voi jakaa verkon liikenteen erillisiin tuotanto- ja tutkimusvuonoihin. Tutkijat voivat hallita omia vuonojaan; valita niissä käytettävät reitit ja prosessit. Tämä antaa heidän kokeilla uusia reititysprotokollia, turvallisuusmalleja (eng: security models), osoitekaavoja (eng: addressing schemes) ja jopa vaihtoehtoja IP-protokollalle, ilman että ne vaikuttavat tuotantoverkon toimintaan. (Mt.)

OpenFlown protokolla

Kuten OpenFlow whitepaper asian kuvailee, OpenFlow on standardoitu kommunikaatiorajapinta, joka on määritelty SDN-arkkitehtuurin kontrolli- ja ohjaustasojen välille. OpenFlow mahdollistaa suoran pääsyn ja mahdollisuuden muokata verkkolaitteiden ohjaustasoa niin fyysisissä kuin virtuaalisissa kytkimissä ja reitittimissä. OpenFlowta voidaankin verrata suorittimen käskykantaan. Protokolla määrittää primitiivit, joita ulkoiset sovellukset voivat käyttää ohjelmoimaan verkkolaitteen ohjaustasoa (eng: forwarding plane) samaan tapaan, kuin suorittimen käskykanta ohjelmoisi tietokonetta. (Ks. kuvio 3.) (ONF SDN New Norm 2012.)



MAC src	MAC dst	IP Src	IP Dst	TCP dport	...	Action	Count
*	10:20:.	*	*	*	*	port 1	250
*	*	*	5.6.7.8	*	*	port 2	300
*	*	*	*	25	*	drop	892
*	*	*	192.*	*	*	local	120
*	*	*	*	*	*	controller	11

Kuvio 3. Esimerkki OpenFlow-käskykannasta

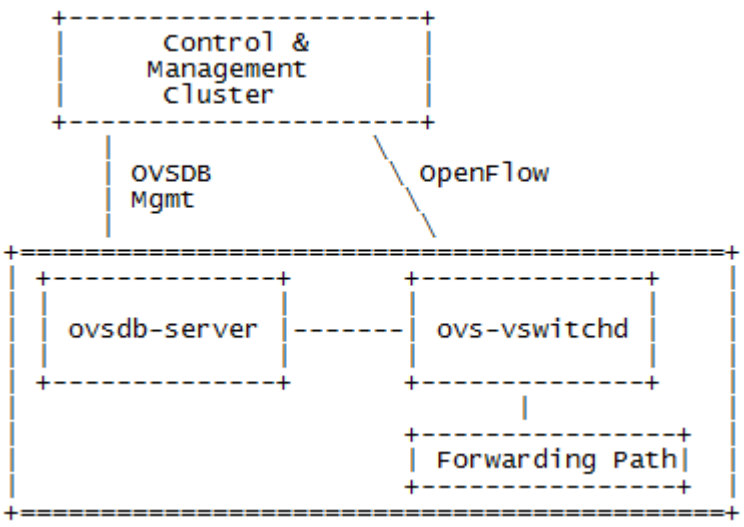
OpenFlow-protokolla implementoidaan molemmille puolille verkkolaitteen ja kontrolleriohjelmiston välistä rajapintaa. OpenFlow käyttää vuo-konseptia tunnistamaan verkkoliikenteen kontrollerin joko staattisesti tai dynaamisesti ennalta määritettyjen sääntöjen perusteella. Se myös mahdollistaa ylläpidolle määrittää, kuinka liikennevuot kulkevat verkkolaitteiden, esimerkiksi yleisten käytön, sovellusten ja pilven resurssien, perusteella. Koska OpenFlow mahdollistaa verkon ohjelmoinnin vuokohtaisesti, OpenFlow-perusteinen SDN-arkkitehtuuri tarjoaa erittäin rakeisen (eng: granual) hallinnan mahdollistaen verkon reaaliajassa vastaamisen muutoksiin sovelluksissa, käyttäjissä ja sessiotasoissa (eng: sessions levels). Nykyään IP-pohjainen reititys ei tarjoa tämän tason kontrollia, sillä kaikki vuot kahden pisteen välillä seuraavat samaa reittiä verkon läpi riippumatta niiden eri vaatimuksista. (Mt.)

OVSDB

OVSDB tai ”Open vSwitch Database Management Protocol” on alkujaan Niciran kehittämä OpenFlow hallintaprotokolla, joka on suunniteltu hallitsemaan Open vSwitch ratkaisuja. Open vSwitch, josta kerrotaan tarkemmin luvussa 6.1, on virtuaalinen kytkinohjelmisto, jota voidaan ajaa joko palvelimella tai fyysisellä kytkimellä olevan hypervisoriksi kutsutun alustan päällä. OVSDB onkin tärkeä osa virtualisoituja SDN ratkaisuja. (What is OVSDB? 2014)

OVSDB:n määritelmä on julkaistu IETF:ssä RFC 7047:nä, jossa OVSDB kuvaillaan seuraavasti: OVSDB-hallintaprotokolla on tarkoitettu mahdollistamaan ohjelmoitavan pääsyn Open vSwitchin tietokantaan, jossa säilytetään konfiguraatioita Open vSwitch daemoniin. Lyhyesti ilmaistuna vaikka OpenFlow edelleen muokkaa ohjaustasoa, muokkaa OVSDB itse virtuaalista kytkintä eli asioita kuten sillat, portit ja rajapinnat. (Pfaff & Davie 2013.)

Kuten RFC 7047:ssä on määritetty (ks. kuvio 4), Open vSwitch-instanssi koostuu tietokantapalvelimesta (ovsdb-server), vSwitch daemonista (ovs-vswitchd) ja vaihtoehtoisesti moduulista, joka suorittaa nopean polun (fast-path) ohjausta. Kontrolli- ja hallintaklusteri (Control & Management Cluster) koostuu jostain määrästä hallintayksiköitä ja kontrollereita. Hallintayksiköt käyttävät OVSDB-hallintaprotokollaa hallitsemaan OVS-instansseja, joista jokaista hallitsee vähintään yksi hallintayksikkö. Kontrollerit käyttävät OpenFlowta asentamaan vuotiloja OpenFlow-kytkimiin. OPV-instanssi voi tukea useita loogisia datareittejä, joita kutsutaan silloiksi. Jokaista OpenFlow-siltaa kohti on vähintään yksi kontrolleri. (Mt.)



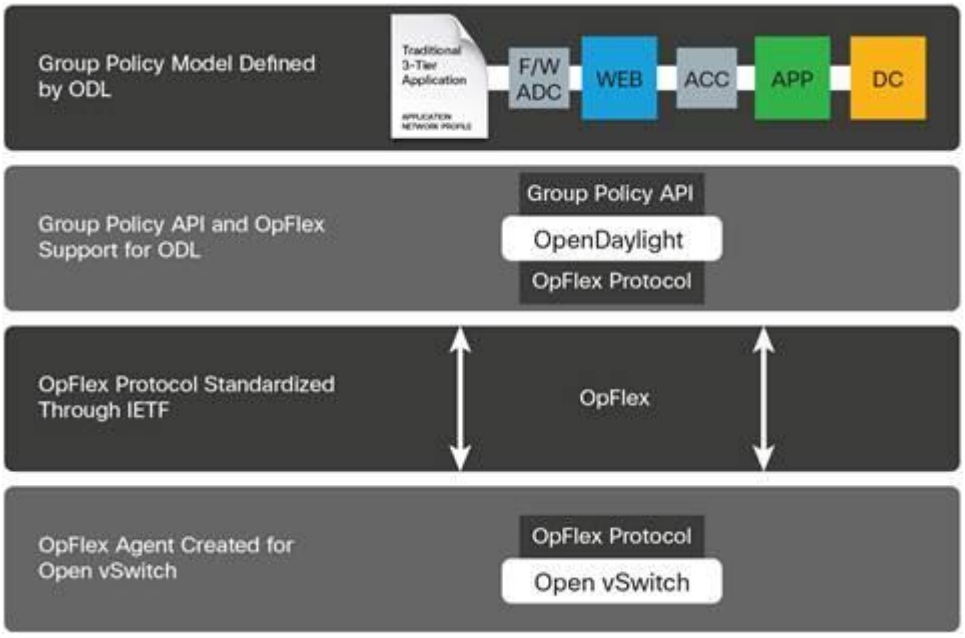
Kuvio 4. Open vSwitchin sekä kontrolli- ja hallintaklusterin pääkomponentit

OVSDB hallintaliittymää käytetään hallinnan ja konfiguroinnin tekemiseen OVS-instanssissa. Verrattuna OpenFlowiin OVSDB-hallintaoperaatioita tapahtuu pitkällä aikavälillä. OVSDB operaatioita ovat muun muassa OpenFlow-datapolkujen sekä niiden porttien ja tunneliliittymien luonti, muokkaus ja poisto, konfigurointi kontrollereille, joihin OpenFlow-datapolut yhdistetään, konfigurointi hallintayksiköille, joihin OVSDB-palvelin yhdistää, QoS-käytäntöjen konfigurointi sekä statistiikan kerääminen. OVSDB ei kuitenkaan suorita vuokohtaisia operaatioita, vaan niistä on vastuussa OpenFlow. (Mt.)

2.4.2 OpFlex

OpFlex on southbound-protokolla, joka on luotu ensisijaisesti Ciscon omaan ACI-nimiseen SDN-ratkaisuun hallitsemaan verkkolaitteita. Ciscon omien sanojen mukaan OpFlex on kasvavaksi suunniteltu protokolla, jonka tarkoitus on vaihtaa abstrakteja käytäntöjä verkkokontrollerin ja ryhmän protokollaa ymmärtävien älykkäiden laitteiden välillä. OpFlex nojaa erilliseen tietomalliin, jota sekä kontrollerit että laitteet ymmärtävät. Tämän tietomallin täytyy perustua abstrakteihin käytäntöihin antaen jokaiselle laitteelle vapauden tehdä käytäntöjä kyseisen abstraktin semanttisten rajojen sisällä. Tästä syystä OpFlex voi tukea mitä vain laitetta mukaan lukien hypervisor-kytkimet, fyysiset kytkimet, sekä tasojen 4 – 7 verkkolaitteet. (Cisco OpFlex 2014.)

Cisco on lähettänyt OpFlexin kommentoitavaksi IETF:lle ja suunnittelee johtavansa myös standardointiprosessia kyseistä reittiä samaan aikaan työskennellessään avoimen lähdekoodin yhteisön kanssa tarjotakseen avoimen lähdekoodin toteutuksen. OpFlex on edelleen tämän kirjoittamishetkellä kehityksessä osaksi OpenDaylight-projektia, jossa sille määritellään yhteistä käytäntömallia. Cisco työskentelee myös avoimen lähdekoodin OpFlex-agentin luomiseksi Open vSwitchille. Ciscon tavoitteena on tarjota yhteisölle kolme pääkomponenttia: avoimen lähdekoodin käytäntöratkaisu, kontrolleripuolen OpFlex-ratkaisu OpenDaylightiin sekä kytkinpuolen OpFlex agentti Open vSwitchiin. (Ks. Kuvio 5.) (Mt.)



Kuvio 5. Yleiskuva OpFlexistä

2.5 Hybridi-SDN

2.5.1 Synty

OpenFlow saattaa tarjota verkolle southbound-ohjelmointirajapinnat, mutta jotkut valmistajat kuten Juniper näkevät SDN:n ensisijaisena etuna verkon käytön ketteryyden ja kyvyn ohjelmoida sen toimintoja ulkoisella kontrollerilla. Nämä valmistajat ovat tunnistaneet esimerkiksi BGP:n potentiaalisena SDN-protokollana, millä mahdollistaa verkon ohjelmoitavuuden jonka SDN on luvannut. Tämä vain osittain OpenFlown tarjoamat ominaisuudet sisältävä toteutus on saanut nimekseen hybridi-SDN. (Johnson 2013a.)

Yksi SDN:n suurimpia ongelmia on perinteisten protokollien kannattajien mielestä kontrollerien yhteen toimimattomuus keskenään. Lisäksi olemassa olevien protokollien käyttö poistaa tarpeen matalan suorituskyvyn yhdyskäytäväohjelmistolle fyysisen ja virtuaalisen puolien yhdistämiseen. (Mt.)

2.5.2 BGP

Hybridi-SDN-ratkaisussa kontrolleri käyttää BGP:tä hallitsemaan verkon reititystä ja NETCONF-protokollaa keskustelemaan fyysisten reitittimien, kytkimien ja verkkopalvelujen kuten palomuurien kanssa. BGP:llä toteutettu SDN toimii usean valmistajan laitteiden välillä, ilman että infrastruktuuria täytyy päivittää lainkaan. Sen avulla pystytään yhdistämään SDN-toimintoja olemassa oleviin logiikkaan ja prosesseihin. BGP ei kykene vuokohtaiseen liikenteen hallintaan, mutta se ymmärtää mm. fyysisten ja virtuaalisten topologioita sekä tietoturvakäytäntöjä. (Johnson 2013a.)

2.5.3 XMPP

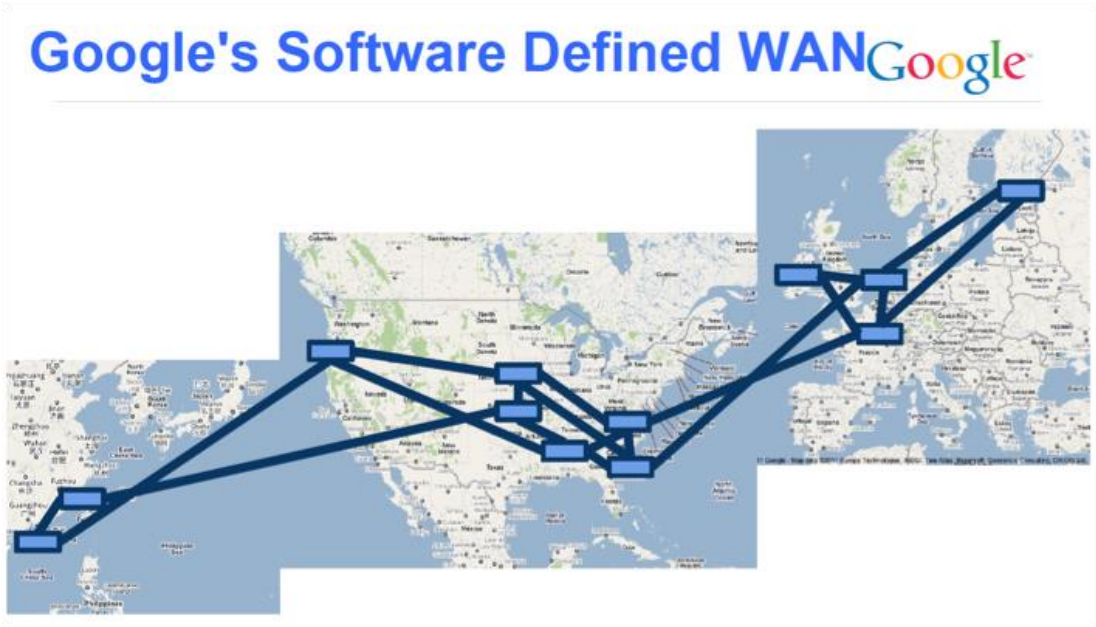
XMPP eli Extensible Messaging and Presence Protocol, joka suunniteltiin alkujaan pikaviestintäprotokollaksi, on saamassa myös jalansijaa southbound-SDN-protokollana. Kontrolleri voi kuljettaa XMPP:llä sekä ohjaustason että hallintatason informaatiota. Perinteisiä protokollia tarvitaan kuitenkin edelleen yhteensopivuuden takaamiseksi vanhojen verkkojen ja järjestelmien kanssa. Sekä Juniper että Arista ovat tutkineet mahdollisuutta XMPP:n käyttämiseksi SDN-ratkaisuissa. (Johnson 2013b.)

Yksi esimerkki XMPP-SDN:stä on Juniperin Contrail-tuote, josta kerron enemmän luvussa 4.4. Juniper käyttää ratkaisussaan overlay-tekniikkaa, jossa SDN voidaan ajaa olemassa olevan verkon päällä, vaikka verkko itsessään ei tarvittavia protokollia tuki-sikaan. Ainakin toistaiseksi kontrollerissa käytetään XMPP:tä kommunikointiin, mutta jatkossa siihen on mahdollista lisätä myös OpenFlow-tuki. (Kerner 2013.)

2.6 Tunnettuja käyttäjiä

2.6.1 Google

Ensimmäinen tunnettu kaupallinen OpenFlown käyttäjä oli Google, jonka ensimmäinen OpenFlow-linkki pystytettiin tammikuussa 2010. Vuoden 2012 alulla koko Googlen sisäinen runkoverkko pyöri OpenFlown päällä (ks. kuvio 6). (Hoezle 2012.) OpenFlown ja tietoliikennesuunnittelun (eng: traffic engineering) ansiosta Google pystyy hyödyntämään verkon kapasiteetistaan jopa 95 %, joka on Googlen mukaan alalla ennenkuulumatonta (Google WAN 2012). Tästä huolimatta Googlella ei pelätä palveluiden heikkenemistä vikatilanteessa, sillä priorisoimalla liikennettä hidastuminen vaikuttaa vain vähemmän tärkeään liikenteeseen (Dix 2012).



Kuvio 6. Googlen SDN-pohjainen runkoverkko (Hoezle 2012)

Googlen WAN koostuu kahdesta osasta; internettiin suuntaava verkko, joka kuljettaa käyttäjien dataa, sekä sisäinen verkko, joka kuljettaa dataa pitkiä matkoja datakeskusten välillä. Näistä kahdesta jälkimmäinen muutettiin OpenFlow-pohjaiseksi SDN:ksi. Projektin alkaessa ei kuitenkaan sopivaa laitteistoa ollut olemassa, vaan Googlen piti kehittää omat kytkimensä. (Mt.)

Googlen on tiedetty rakentavan omia 10GbE kytkimiään jo vuodesta 2007, kun tutkimukset viittasivat siihen, että Google paitsi suunnittelee omat kytkimensä, myös ostaa niihin tarkoitettuja komponentteja (Google 10G switch 2007). Myöhemmin Googlen edustaja on antanut ymmärtää haastattelussa, että heidän lopullinen suunnitelma ei ole ryhtyä laitevalmistajaksi, vaan jatkossa hankkia OpenFlow-yhteensopivat laitteet olemassa olevilta valmistajilta, kunhan niitä on yleisemmin saatavilla (Dix 2012).

2.6.2 Facebook

Facebookin uusi Altoonan datakeskus on rakennettu kokonaan SDN-ajattelun ympärille. Entisten valtavien satojen serverien klusterien, sekä monimutkaisten isojen yhden valmistajan verkkolaitteiden sijaan, Facebook rakensi datakeskuksen pienempien kapselien (pod) ympärille. Jokainen kapseli koostuu 48 TOR-kytkimestä, jotka jokainen yhdistyvät eteenpäin neljään edullisempaan verkkokytkimeen. Tarvittava kaista on laskettu niin, että yksikään laite ei missään vaiheessa ole ylikuormitettu, vaan jokaiselle TOR-kytkimelle on varattu niiden tarvitsema kapasiteetti. (Matsumoto 2014.)

Facebookin datakeskuksen verkko edustaa hybridi-SDN:ää, jossa koko verkon reititys aina TOR-kytkimistä verkon reunalle saakka on toteutettu BGP4/ECMP-protokollilla. Hallinta tapahtuu muiden SDN-ratkaisujen tapaan verkkotasolla kontrollerin toimesta yksittäisten laitteiden sijaan. Facebook on rakentanut omat työkalunsa, joiden avulla konfiguraatiot viedään laitteille missä tahansa topologiassa. BGP-kontrolleri pystyy lukemaan kytkinten reititystietoja ja tarvittaessa automaattinen BGP-reititys voidaan yliajaa verkkopalvelun tarvitsemalla reitillä. Työkaluilla myös mahdollistetaan automaattinen uusien verkon laitteiden ja palveluiden havaitseminen. BGP:lle tyypillisesti myös vioittuneet laitteet havaitaan ja kierretään, kunnes vika on korjattu. (McGillicuddy 2014.)

McGillicuddyn mukaan SDN-ratkaisuksi tavalliselta kuulostavan BGP:llä luodun verkon tekeekin sen ohjelmallisesti keskitetty hallinta. Mitään ei tarvitse hallinnoida käsin ja kaikki määritykset tuodaan ohjelmistolta. Sama pätee myös operointiin, valvontaan ja vianselvitykseen. Uusien laitteiden lisäämisen jälkeen automatiikka pitää huolen roolin selvittämisestä topologian perusteella ja syöttää laitteelle valmiiksi luodun konfiguraation. (Mt.)

3 Tietoturva

3.1 Tietoturva tietoverkoissa

Internetin kehittyessä ja tietoverkoissa kulkevan tiedon määrän kasvaessa on tietoturvalla jatkuvasti suurempi merkitys yritysten toiminnalle. Tietoturvaa parantamalla parannetaan samalla palveluiden luotettavuutta ja vähennetään mahdollisuutta, että yrityksen tuotteiden ja asiakkaiden tietoja leviää ulkopuoleisille. (ONF SDN Security Considerations 2013.)

Open Networking Foundation listaa tämän päivän tietoturvaratkaisuksi seuraavat:

- Palomuurit verkon laidan puolustukseen ja sisäisen domainin hallintaan.
- Tunkeutumisen havaitsemisen (IDS) ja estämisen (IPS) järjestelmät, jotka valvovat verkon toimintoja ja etsivät haitallista toimintaa tai käytäntöjen rikkomista sekä yrittävät ehkäistä hyökkäyksiä.
- SSL VPN eli SSL-suojatut virtuaaliset lähiverkot, jotka tarjoaa turvallisen tavan erottaa asiakkaat ja domainit.
- Verkon hallintaratkaisut, jotka yrittävät keskitetysti hallita monia näitä tietoturvafunktioita konsolin kautta.
- IEEE 802.1X porttipohjainen verkon todennus ja pääsyn hallinta.
- IPsec päästä päähän (eng: end-to-end) todennukseen ja salaukseen IP-paketeille kommunikaatiosessioihin.
- TLS-suojaus sovelluskerroksen kommunikaation suojaamiseksi kuljetustasolla.
- RADIUS-verkkoprotokolla, joka tarjoaa keskitetyn AAA:n eli todentamisen, valtuutuksen ja tilastoinnin loppulaitteille verkkopalvelun käyttämiseen. (Mt.)

3.2 SDN-verkon vaikutuksista

SDN tuo mukanaan huomattavia muutoksia tietoturvaan niin hyvässä kuin pahassa. Omien laitteiden tuominen mukaan verkkoon helpottuu, jolloin myös omien laitteiden kautta tulevat haittaohjelmat yleistyvät. Vastaavasti myös laitteiden asetukset ja

ohjelmistot saadaan helpommin keskitetysti päivitettyä kontrollerilta, mutta mikäli kontrolleri itsessään kaapataan tai jumiutetaan palvelunestohyökkäyksellä, vaarantaa se koko verkon toimivuuden. Uudet käyttötavat, missä tahansa, milloin tahansa, millä laitteella tahansa, aiheuttavat uudenlaisia ongelmia myös perinteisen tietoturvan pystyttämiseen, eikä millään yksittäisellä tekniikalla pystytä tarjoamaan täyttä suojaa. (Mt.)

SDN tarjoaa kuitenkin lukuisia ominaisuuksia auttamaan tietoturvan luomisessa. Vuo-malli on luonnostaan päästä päähän -tyyppinen. Keskitetty hallinta antaa tehokkaan tavan tarkkailla koko verkon suorituskykyä ja mahdollisia uhkia. Käytännöt voidaan määrittää menemään niin sovelluksen, palvelun, organisaation kuin sijainnin mukaan ja niitä voidaan säätää dynaamisesti lennosta. Resursseihin perustuvat tietoturvakäytännöt mahdollistavat erilaisilla riskeillä varustettujen erilaisten laitteiden yhdistetyn hallinnan. Joustavan polkujen hallinnan avulla mahdolliset uhat voidaan eristää verkosta vaikuttamalla muihin verkon käyttäjiin. (Mt.)

Koska SDN sisältää rajapintoja, joilla sovellus voi keskustella verkon kanssa ja tilata tarvitsemiaan palveluita, se voi aiheuttaa myös riskin tietoturvalle tai käytettävyydelle. Verkon tarjoamat palvelut voivat häiritä toisiaan ja vaarantaa verkon toimivuuden. (Mt.)

3.3 Kontrollerin suojaus

SDN-verkon kontrolleri on yksi haavoittuvimpia kohteita SDN-verkossa. Loogisesti keskitetty, vaikkakin fyysisesti hajautettu, kontrolleri on yksittäinen piste, johon kohdistettuna hyökkäykset voivat aiheuttaa vakavaa vaaraa koko verkolle. Yhteyden täytyy olla paitsi siihen, myös siitä verkkolaitteille, erityisen hyvin suojattu. Suojauksella varmistetaan, että vain oikeilta tahoilta tulevat viestit otetaan vastaan verkkolaitteilla mutta myös, etteivät verkolle lähetetyt komennot tai verkolta tuleva data päädy vääriin käsiin. Tämän seurauksena kontrollerin asetusten määritykseen ja sen

suojaukseen tulee kiinnittää erityistä huomiota. (ONF SDN Security Considerations 2013.)

OpenFlow standardi määrittää käytettäväksi TLS- tai UDP/DTLS-suojausta, joista molemmat tukevat tunnistautumista ja salausta. Tärkeää on kuitenkin varmistaa, että verkko kykenee toimimaan myös aikana, kun kontrolleriin ei saada yhteyttä ja että uudet vuot synkronoidaan laitteiden yhteyden palauduttua kontrollerin kanssa. (Mt.)

Esimerkkinä ajan tasalla olevan suojauksen tärkeydestä käy viime aikoina otsikoihin noussut Googlen tutkijoiden tunnistama POODLEksi ristitty hyökkäys, joka mahdollistaa TLS:lläkin suojatuissa verkoissa SSLv3-haavoittuvuuden hyödyntämisen. Hyökkäys perustuu parhaan mahdollisen suojauksen hyödyntämiseen. Kun kommunikaatio palvelun ja asiakkaan välillä epäonnistuu TLS-suojausta käyttäen, pyritään tämän jälkeen käyttämään SSLv3-suojausta. Koska kyseinen suojaus taas on nykyisellään helposti murrettavissa, mahdollistaa tämä esimerkiksi välistävetohyökkäyksen. (Möller & Duong & Kotowicz 2014.)

Ongelman voi kiertää joko poistamalla SSLv3:n kokonaan käytöstä vaarantaen samalla yhteensopivuuden vanhempien järjestelmien kanssa tai ottamalla käyttöön TLS_FALLBACK_SCSV-mekanismin. Kyseinen ominaisuus lisää asiakkaan kättelyviestiin merkinnän, mikäli kättely epäonnistui. Jos kättely menee läpi tämän jälkeen ja palvelin näkee kyseisen merkinnän, se vertaa kättelyssä olevaa SSL/TLS-versiota ja palvelimen korkeinta tuettua versiota toisiinsa. Jos kättelyn versio on matalampi, palvelin katkaisee yhteyden. (POODLE FALLBACK 2014.)

Haavoittuvuuden takia CloudFlare ilmoitti 14. lokakuuta 2014 poistaneensa SSLv3:n oletuksena käytöstä heidän kaikilta asiakkailtaan. Heidän julkaisemien tilastojen mukaan vain 0,09 % kaikesta heidän verkossaan tapahtuvasta liikenteestä ja 0,65 % kaikesta heidän verkon HTTPS-liikenteestä, on suojattu SSLv3 protokollalla. (Prince 2014.)

3.4 Automaattinen haittaohjelmien eristys

Automaattinen haittaohjelmien karanteeni, eli AMQ, havaitsee ja eristää huonosti suojatut verkkolaitteet, ennen kuin ne voivat aiheuttaa haittaa verkon toiminnalle tai muille laitteille. Mahdollisen uhkan paljastuessa AMQ tunnistaa ongelman ja automaattisesti lataa tarvittavat päivitykset sen korjaamiseksi. Tällä aktiivisella lähestymistavalla tietoturvauhat voidaan eristää ja eliminoida tavalla, joka ei normaalisti olisi mahdollista mille tahansa yksittäiselle verkon osalle. (ONF SDN Security Considerations 2013.)

Perinteisissä verkoissa AMQ on yleensä laitevalmistajan omistama ratkaisu, jossa jokainen laite toteuttaa omaa funktiotaan itsenäisesti ja rajoitetulla tietoisuudella muista verkon laitteista. Kyseiset ratkaisut ovat suunniteltu staattisille vuoille, ja niiden täytyy olla kykeneviä valvomaan sisään tulevaa liikennettä. Kyseinen suljettu lähestymistapa on kuitenkin joustamaton erityisesti datakeskuksissa, joissa palvelinten kuormitus on virtualisoitu, liikennevuot muuttuvat ja useita samanaikaisia käytäntöjä täytyy ylläpitää. Suuremmat 40G- ja 100G-linkit tekevät ympäristöstä entistäkin haastavamman. (Mt.)

OpenFlow-pohjainen verkko tarjoaa joustavamman lähestymistavan, jossa AMQ:n toiminnollisuus on keskitetty SDN-kontrollerille. Kontrollerista käsin AMQ voi tarjota tehokkaan tietoturvan prosessoinnin, kun ainoastaan epäilyttävät vuot eristetään ja otetaan tarkkailun alle. Vuopohjaisen mallin tekee erityisen hyväksi AMQ:n kannalta sen kyky hallita rakeisia käytäntöjä ja palveluketjuja. (Mt.)

4 SDN-ratkaisut

4.1 Cisco ACI

SDN:n ympärillä pyörivä pörinä luo painetta Ciscolle, jonka korttipalvelimien markkinaosuuden kasvusta huolimatta, reitittimien ja kytkimien tilanne näyttää jatkuvasti heikommalta. Vuonna 2013 raportoitiin Ciscon miljardin dollarin sopimuksen Amazonin kanssa verkkolaitteiden myymisestä romuttuneen, kun Amazon päätti sen sijaan ostaa vain 11 miljoonalla dollarilla edullisempia verkkolaitteita ja täyttää muut tarpeet SDN:llä. Tämän lisäksi Cisco selvitti miten heidän liikevaihdolle kävisi, jos Cisco siirtyisi SDN-markkinoille. Loppupäätelmä oli, että heidän toiminnan arvo noin puolittuisi 43 miljardista dollarista 22 miljardiin. (Bort 2013.)

SDN-buumiin vastatakseen Cisco rahoitti uuden yrityksen perustamisen, jonka tarkoituksena kehittää uusi SDN-tyyppinen ratkaisu Ciscon perinteisten tuotteiden tueksi. Vuonna 2012 Cisco rahoitti kolmen jo aiemmin menestyneen insinöörin perustaman Insieme-nimisen spin-in yrityksen. (Malik 2012.)

Ciscon aiempi yritys SDN-markkinoille oli ONE-kontrolleri ja -ympäristö, julkaistu huhtikuussa 2012. Se tukee Ciscon omaa onePK (ONE Platform Kit) -työkalua, joka mahdollistaa omien sovellusten kehittämisen Ciscon reitittimille ja kytkimille käyttämällä yleisiä ohjelmointikieliä mukaan lukien C, Java ja Python. onePK on saatavilla sekä uusille NX-OS sekä vanhemmille IOS ja IOS XR -alustoille. ONE-kontrolleri tuki myös OpenFlow-protokollaa. (Cisco onePK 2014.)

Maaliskuussa 2014 Ciscolla olikin julkaista uusi Insiemen kehittämä kontrolleri, APIC. Kontrolleri on osa Ciscon ACI-ympäristöä, jossa se on ainut paikka, jossa verkon käytäntöjä tarvitsee ohjelmoida. Myös käytäntöjä on tarkoitus yksinkertaistaa. APIC on suunniteltu yhteensopivaksi Ciscon vanhempien tuotteiden kanssa. Sen tarkoitus on

korvata osittain Ciscon aiemmin tukema OpenDaylight-kontrolleri, XNC, joka jää elämään Ciscon SDN-ratkaisuna muiden valmistajien laitteita varten. (Matsumoto 2014.)

ACI-ympäristö ja APIC-kontrolleri hyödyntävät Ciscon kehittämää OpFlex-protokollaa, joka julkaistiin huhtikuussa 2014. OpFlex toimii myös osana Ciscon omaa ONE-kontrolleria. OpFlex on myöhemmin otettu myös osaksi useita avoimia projekteja, kuten OpenDaylight ja OpenStack. (Duffy 2014.)

Ciscon mukaan ACI eroaa OpenFlown mallista olemalla deklaratiivinen (selittävä), kun OpenFlow on imperatiivinen (määräävä). Deklaratiivisen mallin alla sovelluskäytännöt abstraktoidaan verkosta kontrollerille, mutta toisin kuin perinteisessä SDN-mallissa, niiden tulkinta ja määrittäminen jätetään laitteiden vastuulle. Kun ACI-verkko saa sovelluskäytännön sen APIC-kontrollerilta, verkkolaite päättää kuinka se konfiguroi itsensä, sen sijaan että se jättäisi configuraation kontrollerille. Ciscosta sanotaan, että tämä tekee APIC:stä kattavamman kaikille verkon laitteille ja yksinkertaistaa uuden infrastruktuurin integroimista asiakkaan olemassa oleviin järjestelmiin. Ratkaisu mahdollistaa myös ACI-verkon nykyisiä SDN-ratkaisuja skaalautuvamman ja resilientimmän tason. (Mt.)

Cisco lisää, että imperatiivisessa SDN-mallissa sovellukset, operaatiot ja infrastruktuurin vaatimukset on kaikki käännettävä verkon konfiguraatioiksi. Tämä aiheuttaa kontrollerin muuttumisen pullonkaulaksi, sen hallinnoidessa jatkuvasti kasvavaa verkkoa. Sovellusten kehittäjien täytyy myös edelleen kuvailla vaatimukset matalalle tasolle, rajoittaen helppokäyttöisyyttä. Ciscon mukaan perinteinen SDN tukee ”pienintä yhteistä nimittäjää”, kuten siltoja, portteja ja tunneleita eri valmistajien ympäristöjen välillä. (Mt.)

Cisco sanoo deklaratiivinen mallin skaalautuvan hyvin, linjaa hyvin sovellusten työtaakan vaatimuksien kanssa ja olevan verrattain helppo hallita. Kuitenkin mm. analysointiyhtiö IDC:llä nähdään, että malli palvelee enemmän Ciscon tarvetta säilyttää

verkkolaitteiden omaa älykkyyttä ja arvoa, kun OpenFlow-mallissa kytkimen älykkyys on rajattu pelkästään pakettien ohjaamiseen. (Mt.)

Nykyään valtaosa tietoturvakäytännöistä määritellään käsin. Gartnerin mukaan vuonna 2018 yli 95 % palomuurien läpäisyistä tulevatkin johtumaan väärästä konfiguraatiosta, ei niinkään virheestä itse palomuurissa. Automatiikan puutteen lisäksi yksi vääriin konfiguraatioihin johtava päätekijä on käytäntöjen laitekeskeisyys ilman kontekstia niitä käyttäviin sovelluksiin. Suuremmissa yhtiöissä voi olla kymmenistä tuhansista miljooniin ACL- ja palomuurisääntöjä. Nämä usein jäävät poistamatta joko toimintamallien puutteen takia tai pelosta syntyviä ongelmia kohtaan. Tämä taas aiheuttaa haasteita niin verkon tietoturvalle kuin sen auditoinnille. (Cisco ACI Security 2014.)

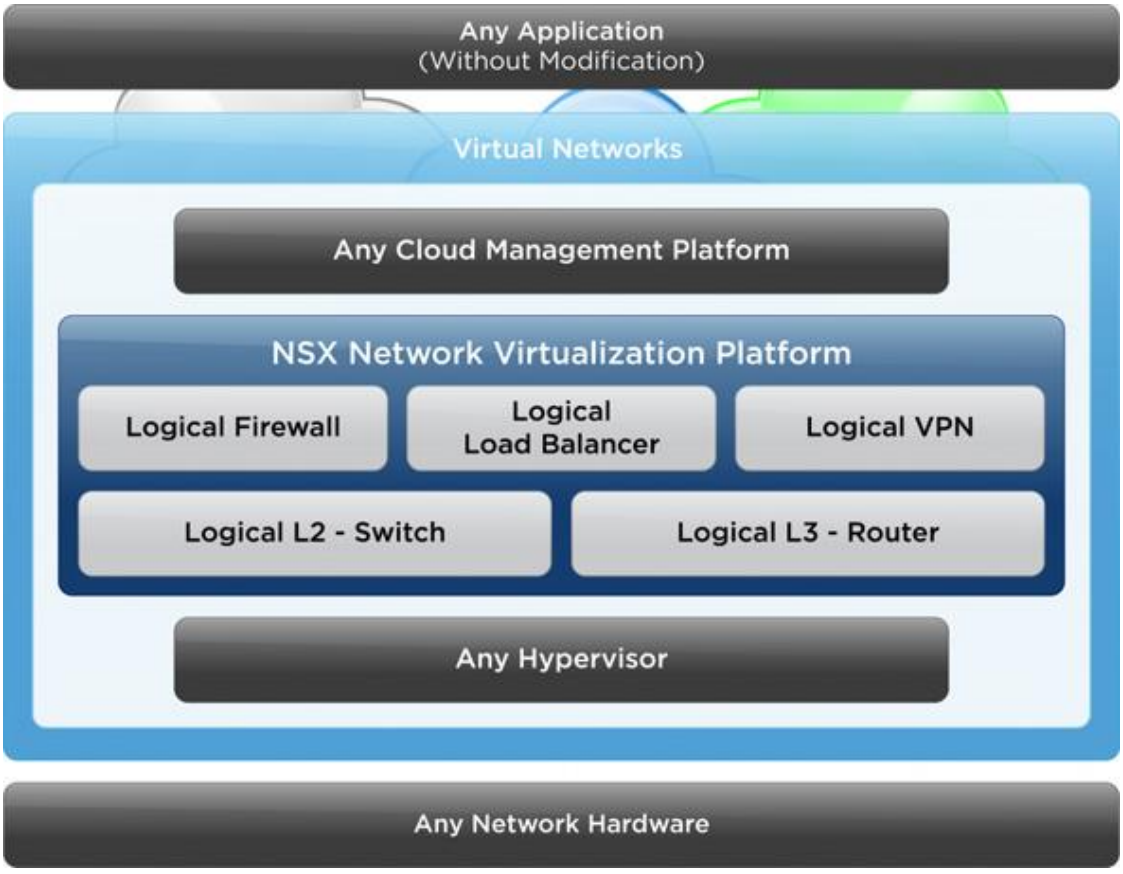
4.2 VMware NSX

VMware NSX on verkon virtualisointiin ja turvallisuuteen keskittyvä alusta ohjelmistolla määritetyille datakeskuksille. NSX mahdollistaa virtuaalisten verkkojen luomisen, tallentamisen, poistamisen ja palauttamisen tarpeen mukaan ilman minkäänlaista fyysisen verkon uudelleenmäärittämistä. Seurauksena datakeskukselle saadaan käyttöön kaikki SDN-mallin hyödyt, ilman työläitä ja mahdollisesti kalliita verkon muutostöitä. NSX toimii missä tahansa IP-verkossa eikä sen tarvitse vaikuttaa verkon päällä oleviin sovelluksiin millään tavalla. (VMware NSX 2013.)

NSX vSwitch on suoraan yhteensopiva monien nykyisten hypervisoreiden kanssa, kuten Xen, KVM ja VMware ESXi. Tarvittaessa tukea voidaan myös laajentaa muihin, kuten Microsoftin Hyper-V:hen, määrittelemällä ne standardin vSwitch kapasiteetin mukaisiksi. Sovellusten verkko- ja tietoturvapalvelut jaellaan hypervisoreille ja ”liitetään” yksittäisiin virtuaalikoneisiin verkko- ja tietoturvakäytäntöjen mukaisesti. Kun virtuaalikonetta siirretään laitteelta toiselle, sen verkko ja turvapalvelut liikkuvat sen

mukana. Mikäli uusia virtuaalilaitteita tarvitaan sovellusta varten, sille lisätään myös dynaamisesti kaikki tarvittavat käytännöt. (Mt.)

Verkon laidalla olevalle hypervisorille asetettu NSX-vSwitch käsittelee paikallisten virtuaalikoneiden väliset linkit. Jos yhteyttä ulospäin tarvitaan, tarjoaa vSwitch yhteyden fyysiseen verkkoon. NSX vSwitch voi tarvittaessa toimia myös reitittimenä tai palomuurina. NSX-kontrolleri sisältää northboud-ohjelmointirajapinnat joilla keskustella sovellusten kanssa. Kun sovellus tarvitsee jotain, ohjelmoi kontrolleri kaikki NSX:n alaisuudessa olevat vSwitchit southbound-suuntaan vastaamaan ilmaistuihin tarpeisiin (ks. kuvio 7). NSX-kontrolleri osaa käyttää ohjelmointiin OpenFlow-protokollaa, mutta se ei ole ratkaisun avainosa. (Banks 2014.)



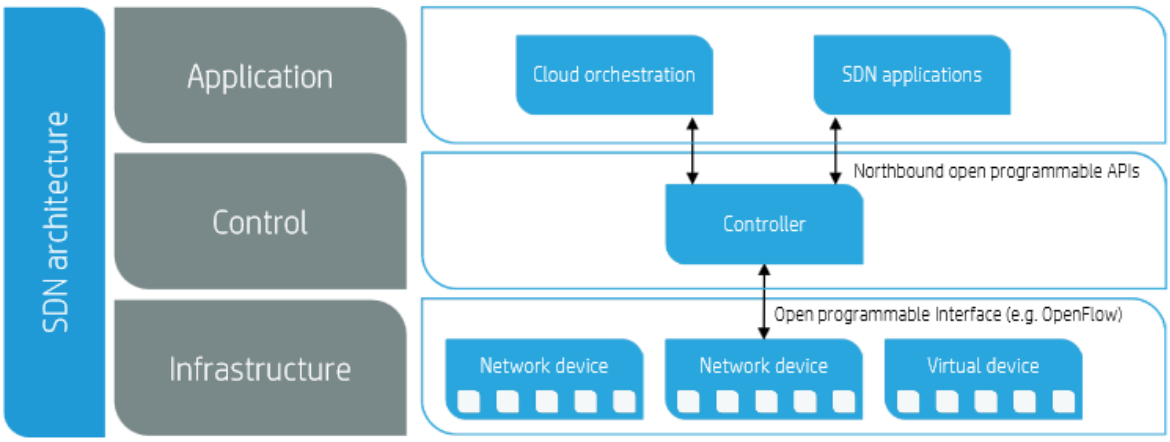
Kuvio 7. VMware NSX kerroksittain

NSX-ratkaisussa tietoturva on toteutettu hajautetulla palomuurilla (eng: distributed firewall), joka saa käytäntönsä keskitetysti kontrollerilta (Banks 2014). Hajautettu palomuuri sijaitsee palveluna jokaisessa hypervisorissa ja jokainen hypervisorista lähtevä tai siihen saapuva paketti kulkee sen läpi. Tämä ratkaisu eroaa merkittävästi perinteisistä fyysisistä tai virtuaalisista palomuureista, sillä kaikkea liikennettä ei enää tarvitse kierrättää verkossa sijaitsevan yhden tai useamman palomuurin läpi. Etuina mm. ehkäistään pullonkaulojen syntymistä, yksinkertaistetaan liikenteen reittejä. sekä varmistetaan palomuurisääntöjen yhdenmukaisuus. (Hedlund 2013.)

4.3 HP SDN

4.3.1 HP VAN SDN

HP kuvailee SDN:n mukaillen ONF:n määritelmää fyysiseksi verkon kontrollitason erottamiseksi ohjaustasosta, jossa yksi kontrolleri voi hallita useita laiteitta. SDN myös mahdollistaa virtuaalisten ja fyysisten ympäristöjen yhdistämisen ja oikein tehtynä avaa ennen näkemättömän kyvykkyyden, älykkyyden ja läpinäkyvyyden. HP:n näkemys loogisesta SDN:stä eroaa perinteisestä lähinnä pilviorkestroinnin erottelulla muista sovelluksista (ks. kuvio 8). (HP SDN NV 2014.)



Kuvio 8. HP:n näkemys loogisesta SDN:stä

SDN-leikkiin HP lähti joulukuussa 2011, kun HP:n kytkimiin julkaistiin vapaasti ilman erityistä lisenssiä ladattava OpenFlow-yhteensopiva ohjelmisto (HP OpenFlow Firmware 2011). HP:n ensimmäinen oma SDN-kontrolleri oli HP Virtual Application Networks SDN Controller, tai HP VAN SDN-kontrolleri, jonka he julkistivat lokakuussa 2012.

HP:n omien sanojen mukaan, se on ohjelmisto, joka tarjoaa keskitetyn hallinnan OpenFlow-kykeneville verkoille. Se myös mahdollistaa uuden sukupolven sovellus-pohjaisia verkkopalveluita ja tarjoaa avoimet ohjelmointirajapinnat kolmannen osa-puolen kehittäjille. HP VAN SDN -kontrolleri on suunniteltu toimimaan kampuksilla, datakeskuksissa ja palveluntarjoajien ympäristöissä. Se sisältää muun muassa proaktiivisen ja reaktiivisen vuoprosessoinnin, graafisen käyttöliittymän, northbound-ohjelmointirajapinnat, OpenFlow-standardin mukaisen TLS-suojauksen, sekä joustavan pakettikäsittelyn niin OpenFlow- kuin perinteisille paketeille. (HP VAN SDN 2014.)

4.3.2 HP VMware Networking solution

HP toi elokuussa 2014 saataville VMwaren kanssa yhteistyönä luodun HP-VMware verkkoratkaisun. Ratkaisu tarjoaa yhdistetyn fyysisen fyysisten ja virtuaalisten verkkojen automaation ja läpinäkyvyyden. Ratkaisu koostuu HP VAN SDN-kontrollerista, HP ConvergedControl SDN-sovelluksesta, HP FlexFagric 5930 kytkimestä ja VMware NSX verkon virtualisointialustasta. OVSDB on käytössä Open vSwitch instanssien hallinnassa. (HP-VMware 2014.)

4.3.4 HP SDN App Store

HP julkaisi ensimmäisenä markkinoille oman SDN-sovellusten verkkokaupan syyskuussa 2014. Sovelluskaupan sovellukset on luokiteltu eri kehille. Ylimpänä ovat HP:n omat sovellukset, jotka ovat HP:n rakentamia ja testaamia. Tämän jälkeen tulevat

HP:n testaamat Premium-kehän sovellukset, kehittäjien testaamat ja HP:n hyväksymät Partner-kehän sovellukset, sekä Community-kehän avoimet yhteisön tukemat sovellukset. (HP SDN App Store 2014.)

Esimerkkejä julkaisussa saatavilla olevista sovelluksista ovat vaikkapa HP Network Protector, joka tarjoaa automatisoidun verkon laitteiden tietoturvan analysoinnin (eng: posture checking) ja tarjoaa reaaliaikaista tietoturvaa ympäri OpenFlow-verkkoja, F5 BIG DDoS Umbrella, joka mahdollistaa asiakkaan implementoida verkon, sovellusten, DNS:n ja SSL:n DDoS-suojauksen verkon reunalle, sekä GuardiCore Defense Suite skaalautuvaan SDN-pohjaiseen verkon tietoturvaan ohjelmallisesti määritettyihin datakeskuksiin, jonka tarkoitus on havaita kehittyneempiä uhkia jo alkuvaiheessa (Mt).

Kokonaisuudessaan HP:n App Store sisälti kirjoitushetkellä kaksikymmentä valmista sovellusta sekä jokusen beta-asteella olevan. Hinnat vaihtelevat HP:n omissa sovelluksissa tuhannen euron kertamaksusta tuhansien eurojen vuosittaiseen maksuun. Yhteistyökumppanien ja yhteisön sovellukset ovat ilmaisia. Tilaaminen onnistuu Yhdysvalloissa helposti sovelluskaupan sisällä, mutta muualla maailmassa se edellyttää yhteydenottoa HP:n myyjään. (SDN App Store 2014.)

4.4 Juniper Contrail

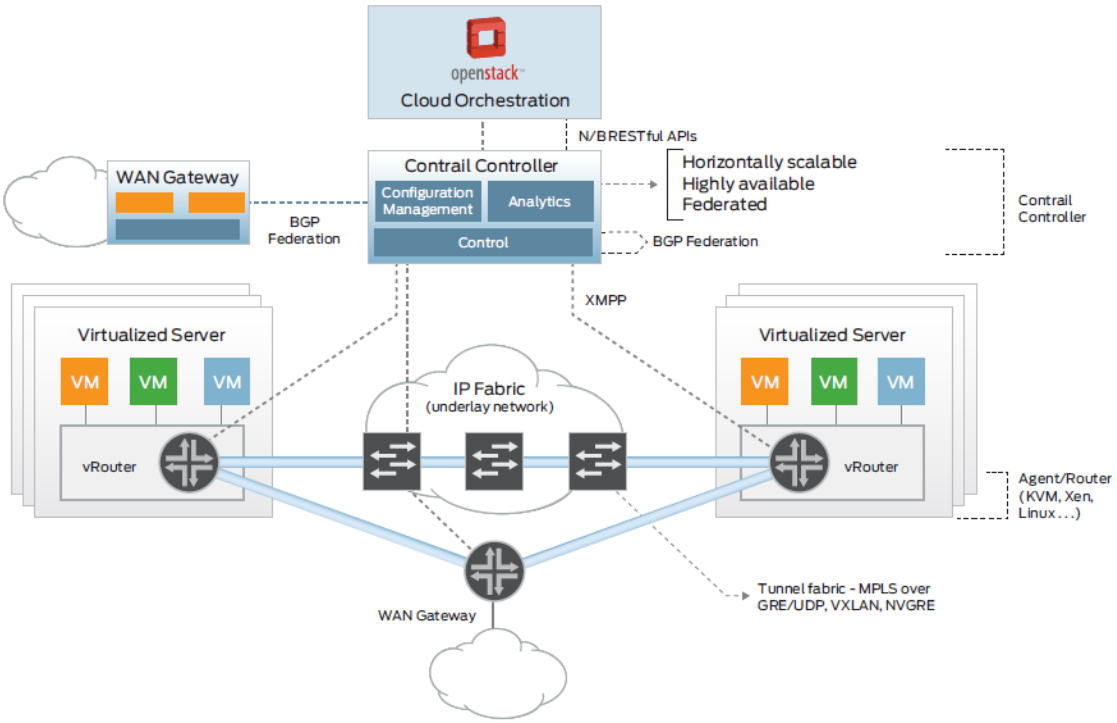
4.4.1 Contrail Networking

Contrail-kontrollerin kehitti samanniminen startup-yritys, jonka Juniperin osti vuonna 2012 (Kerner 2013). Contrail Networking on yksinkertainen, avoin ja joustava pilviverkkojen automatisointituote, joka hyödyntää SDN-teknologiaa orkestroimaan hyvin skaalautuvien virtuaalisten verkkojen luontia. Tuotteen tarkoituksena on tarjota kokonaisvaltainen paketti yrityksen verkon tuomiseksi pilviajalle, mutta jonka voi ottaa

käyttöön korvaamatta kaikkea yrityksen omistamaa arvokasta laitteistoa ja osaamista. Contrail Networking toimii OpenStack-pilviorkestrointialustan kanssa. Se helpottaa pilviarkktitehtuuriin siirtymistä tarjoamalla virtualisoidun verkkokerroksen, joka antaa kytkentä-, reititys- ja verkkopalvelut aiemman fyysisen verkon päällä. Se myös tarjoaa ohjelmointirajapintayhteensopivuuden julkisiin pilviin kuten Amazon Web Servicesiin. (Contrail Networking 2014.)

Contrail Networking koostuu seuraavista osista (ks. kuvio 9):

- Contrail-kontrolleri, joka integroi OpenStack-pilviorkestrointialustan sekä palveluntarjoajan operaatiotukijärjestelmien kanssa. Kontrolleri istuu orkestrointijärjestelmän ja verkkolaitteen välissä, ja keskustelee julkaistun REST-ohjelmointirajapinnan avulla. Kontrolleri hyödyntää verkkolaitteiden hallintaan BGP ja XMPP -protokollia.
- Contrail Networking vRouter, joka varmistaa natiivien L3-tason palveluiden pääsyn virtuaalikoneille. (Mt.)



Kuvio 9. Contrail Networking -ratkaisun looginen näkymä

4.4.2 OpenContrail

OpenContrail on Apache 2.0 -lisenssin alla julkaistu avoin projekti, joka perustuu Juniperin julkaiseman kaupallisen Contrail-alustan lähdekoodiin ja julkaistiin samaan aikaan kaupallisen alustan kanssa. OpenContrail tarjoaa kaikki tarvittavat komponentit verkon virtualisointiin. Osiin kuuluu SDN-kontrolleri, virtuaalinen reititin, analytiikkamoottori (eng: analytics engine), sekä julkaistut northbound-ohjelmointirajapinnat. Kuten kaupallinen Contrail, eroaa projekti muista SDN-kontrollereista sen tavasta hyödyntää perinteisiä hyväksi havaittuja ja todistettuja protokollia, kuten BGP ja MPLS. Ilmaisen projektin tarkoituksena on tukea Contrailin kehitystä ja käyttöönottoa. (OpenContrail FAQ 2014).

5 SDN Kontrollerit

5.1 OpenDaylight

5.1.1 Historiaa

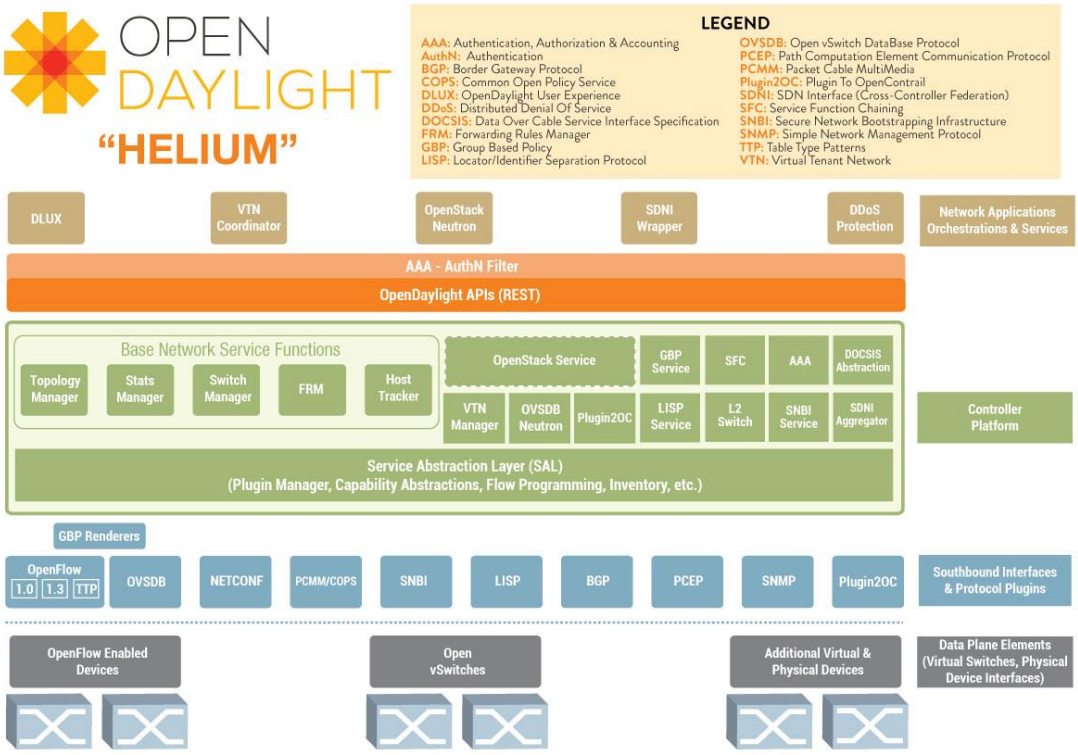
OpenDaylight sai alkunsa huhtikuussa 2013 useiden tahojen yhteistyössä perustettuna projektina avoimen lähdekoodin SDN ja NFV kontrolleriksi. Projekti pyrkii erottumaan avoimuudellaan ja sitä kautta tarjoamaan turvallisuutta ja uusia innovaatioita nopeasti kehittyville SDN-markkinoille. Mukana olivat mm. Cisco Systems, VMware, Juniper Networks, Ericsson ja Linux Foundation. (Lawson 2013.)

Välittömästi perustamisensa jälkeen OpenDaylightiin on kohdistunut myös useita epäilyjä. Vaikka OpenDaylight on ensisijaisesti OpenFlow kontrolleri, ei sen takana oleva Open Networking Foundation ole mukana projektissa. Myöskin Ciscon osallistuminen ja heidän oman ONE-kontrollerin puskeminen osaksi projektia de-facto kontrolleriksi herätti huolta, varsinkin ottaen huomioon Ciscon vielä julkaisematto-man tulevan kilpailevan ACI-ratkaisun. (Duffy 2013.)

OpenDaylightin yhtenä tarkoituksena on yrittää standardoida northbound-ohjelmointirajapinnat verkkoinfrastruktuurista SDN orkestrointitasolle auttaakseen verkon ohjelmointia. OpenFlow on yksi southbound-verkon kontrollointiprotokollista, jota sekä OpenDaylight että ONF tukevat, mutta ONF päätti jättää määrittämättä sille northbound-ohjelmointirajapintoja, eikä sillä ole standardoituja avoimen lähdekoodin tahoja, jotka tätä tekisivät. Tämän seurauksena OpenDaylight päätti ottaa tehtäväkseen kehittää kyseiset de-facto-rajapinnat. Jotkut analyytikot uskovatkin, että OpenDaylight on suunnattu enemmän yhtiöiden käyttöön, kun taas ONF on perustettu suurien webskaalan yritysten ja palveluntarjoajien toimesta ja käyttöön. (Mt.)

5.1.2 Kerrokset ja toiminta

Korkeammalta tasolta katsottaessa SDN kuvaillaan yleisesti kerroksina. Kuviossa 10 voi nähdä OpenDaylightin osat ja kerrokset kokonaisuudessaan. Uusin versio ”Helium” julkaistiin syyskuussa 2014. (Technical Overview 2014.)



Kuvio 10. OpenDaylight Heliumin osat

Verkkosovellukset ja orkestrointi: Ylin kerros koostuu sovelluksista, jotka kontrolloivat ja valvovat verkon käyttäytymistä. Tämän lisäksi siihen kuuluu monimutkaisemmat ratkaisuorkestrointisovellukset pilven ja NFV:n tarpeisiin, sekä palveluiden yhdistäminen ja verkkoliikenteen suunnittelu ympäristöjen tarpeiden mukaisiksi. (Mt.)

Kontrollerialusta: Keskimmäinen kerros tarjoaa kehyksen, johon SDN-abstraktiot voidaan luoda. Kehys tarjoaa myös ylöspäin (northbound) sarjan yleisiä ohjelmointirajapintoja sovelluskerrokselle, sekä alaspäin (southbound) yhden tai useampia protokollia komentamaan ja kontrolloimaan fyysistä laitteistoa verkon sisällä. (Mt.)

Fyysiset ja virtuaaliset verkkolaitteet: Alin kerros koostuu verkon fyysisistä ja virtuaalisista laitteista; kytkimistä, reitittimistä, jne., jotka ovat vastuussa kaikista kytköksistä verkon päätepisteiden välillä. (Mt.)

OpenDaylight on avoimen lähdekoodin projekti, jossa on modulaarinen, liitännäisiä tukeva ja joustava kontrollerialusta sen ytimessä. Tämä kontrolleri on implementoitu tiukasti ohjelmistona ja rajattu omaan Java virtuaalikoneeseensa. Sellaisenaan se voidaan ottaa käyttöön millä tahansa Javaa tukevalla laitteistolla ja käyttöjärjestelmällä. (Mt.)

Northbound-ohjelmistorajapintoihin kuuluvat OSGi, jota käytetään kontrollerin kanssa samassa osoiteavaruudessa oleviin ohjelmiin, sekä webpohjainen REST, jota käytetään sovelluksille, jotka ovat eri osoiteavaruudessa tai kokonaan eri koneella kuin kontrolleri. Logiikka ja algoritmit sijaitsevat sovelluksissa. Nämä sovellukset käyttävät kontrolleria keräämään tietoa verkosta, suorittamaan verkkoanalyysialgoritmeja ja tämän jälkeen käyttävät kontrolleria orkestroimaan uusia sääntöjä ympäri verkkoa. (Mt.)

Southbound-liittymä tukee useita protokollia erillisinä liitännäisinä. Näihin kuuluvat mm. OpenFlow 1.0, OpenFlow 1.3 ja BGP-LS. Nämä moduulit ovat dynaamisesti linkitetty SAL-kerrokseen, joka altistaa laitepalvelut niille niiden yläpuolella oleville moduuleille, joille ne on kirjoitettu. SAL päättää kuinka pyynnöt palveluihin täytetään riippumatta alla olevasta protokollasta kontrollerin ja verkkopalvelun välissä. (Mt.)

5.2 Project Floodlight

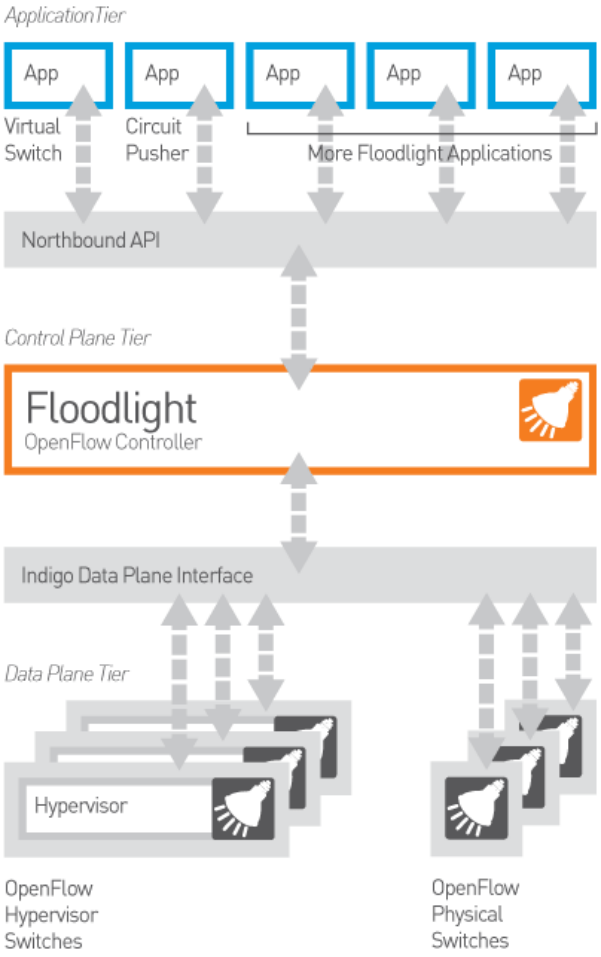
5.2.1 Floodlight-kontrolleri

Floodlight on OpenFlow-protokollaa käyttävä avoin SDN-konrolleri. Se toimii OpenFlowta tukevien reitittimien ja niin fyysisten ja virtuaalisten OpenFlow-kytkimien kanssa. Floodlight on rakennettu Javan päälle. Se on suunniteltu helppokäyttöiseksi ja on laajennettavissa moduuleilla, sekä tukee OpenStack-pilvialustaa. (Floodlight 2014.)

Floodlightia on kehitetty täysin avoimessa yhteisössä ja se onkin julkaistu Apache-lisenssin alla, tehden siitä lähes täysin vapaasti käytettävän missä tahansa tuotteessa tai projektissa. Se toimiikin ytimenä muun muassa Big Switch Networksin ratkaisussa, joka on aktiivisesti kehitetty kaupallinen ratkaisu. (Mt.)

Mikäli Floodlightia haluaa testata, on se helposti ja nopeasti ajettavissa Mac OS X tai Linux-ympäristöissä. Tarjolla on myös valmis Floodlight-virtuaalikone, eli kuva valmiiksi asennetun käyttöjärjestelmän kiintolevystä, jonka saa avattua VMware Fusionilla tai VirtualBoxilla. Virtuaalikone sisältää suoraan asennetun Floodlight-kontrollerin, että OpenFlow-yhteensopivan Mininetillä toteutetun simuloidun OpenFlow-verkon. (Floodlight Getting Started 2014.)

Floodlight-ratkaisu koostuu seuraavista kerroksista (ks. kuvio 11): sovelluskerros, northbound-ohjelmointirajapinnat, Floodlight-kontrollerikerros, Indigo-rajapinta, sekä datakerros virtuaalikytkinten hypervisoreille ja fyysisille OpenFlow-kytkimille (Floodlight 2014).



Kuvio 11. Floodlight-kontrolleri kerroksittain

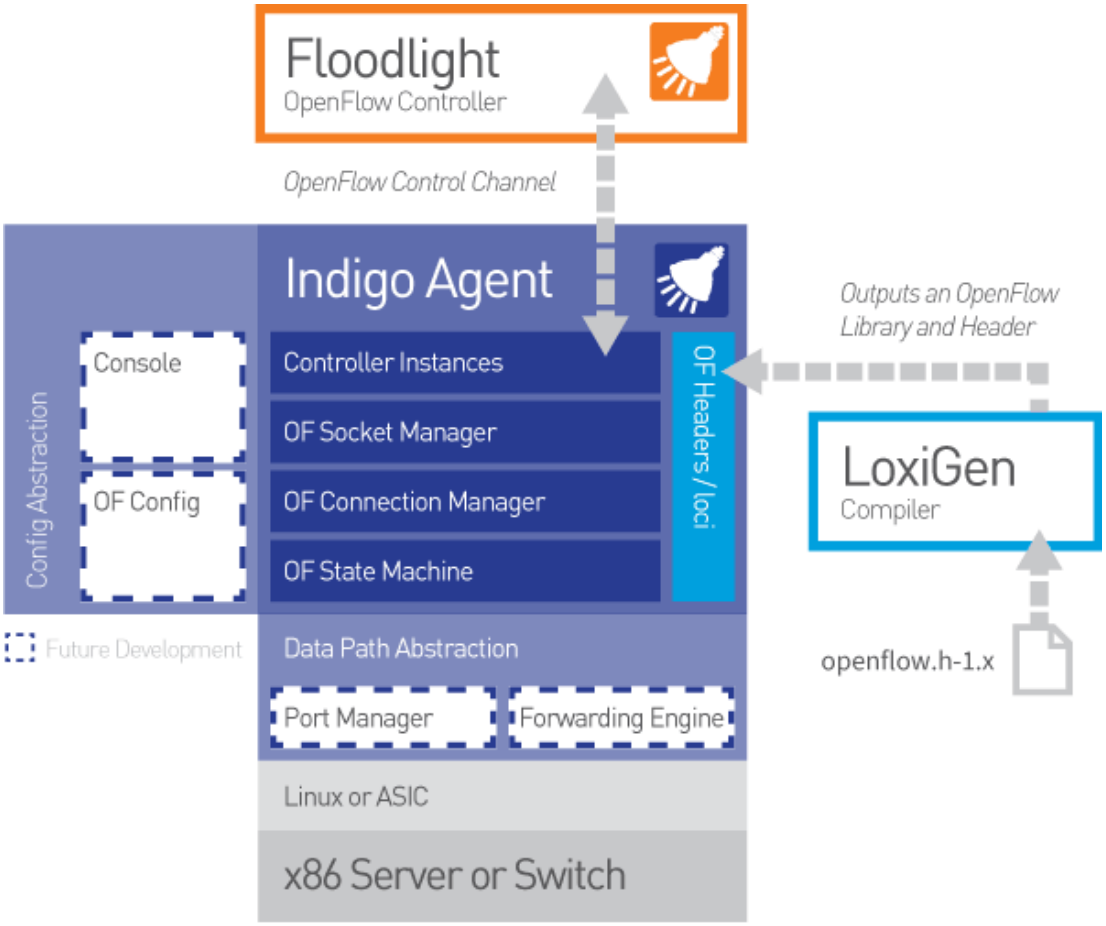
5.2.2 Indigo

Indigo on avoimen lähdekoodin projekti, tarkoituksenaan lisätä OpenFlow-tuki fyysisille kytkimille ja virtuaalikytkinten hypervisoreille. Indigo on myös pohja Big Switch Networksin Switch Light -tuotteelle. (Floodlight Indigo 2014.)

Indigo Agent asettuu Floodlight-ratkaisussa heti kontrollerin alapuolelle. Se kuvaa ydinkirjastoja ja sisältää HAL-abstraktiokerroksen helpottamaan integroimista fyysisten ja virtuaalisten kytkimien porttien ja ohjauksen kanssa, sekä konfiguraatioabstraktiokerroksen tukemaan OpenFlown ajamista ”hybridi” tilassa kytkimessä. (Mt.)

LoxiGen on kääntäjä, joka generoi kirjastoja OpenFlown jäsentämiseen (eng: marshalling) usealla eri kielellä. Nykyään tuettuna kielistä on ainoastaan Loci-niminen C-variantti, mutta Java ja Python ovat kehityksen alla. (Mt.)

Indigo Agent koostuu lukuisista osista, jotka ovat nähtävissä kuviossa 12.

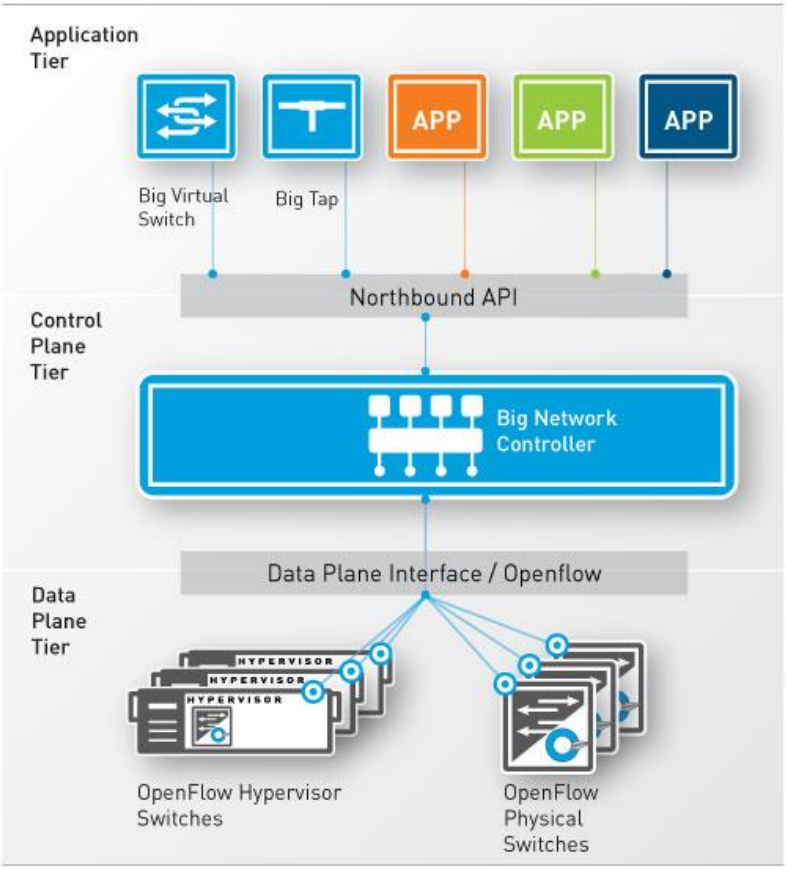


Kuvio 12. Indigo Agentin osat

5.3 Big Network Controller

Big Network Controller on kaupallinen OpenFlow-kontrolleri joka perustuu Project Floodlightiin ja hyödyntää alan standardeja protokollia kuten OpenFlowta. Yhdistettynä avoimiin ja julkaistuihin ohjelmointirajapintoihin, voi Big Network Controller tarjota joustavan ja skaalautuvan alustan verkkosovellusten tuomiseksi. (Big Network Controller 2014.)

Kuviossa 13 nähdään kuinka Big Network Controller ohjelmoi OpenFlow-yhteensopivia laitteita ja altistaa REST-ohjelmointirajapinnan Big Switch Networksin sovelluksille. Controlleri sijaitsee SDN-mallille tyypilliseen tapaan sovelluskerroksen ja datakerroksen välillä.



Kuvio 13. Big Network Controller

6 Kytkimet

6.1 Open vSwitch

Open vSwitch on avoin virtuaalinen monikerroksinen (eng: multilayer) kytkin, joka tarjoaa tuen useille alan standardeille hallintaliittymille ja protokollille, kuten NetFlow, sFlow, SPAN, RSPAN, CLI, LACP ja 802.1ag. Se on kirjoitettu alustariippumattomalla C-kielellä ja suunniteltu toimimaan niin erillisissä reitittimissä, kuin myös käyttämään tietokoneen verkkoportteja. Se toimii siis sekä fyysisissä että virtuaalisissa alustoissa. (Open vSwitch FAQ 2014.)

Open vSwitch on rakennettu ajettavaksi millä tahansa Linux-pohjaisella virtualisointialustalla (kernel 2.6.32 ja uudemmat) mukaan lukien KVM, VirtualBox, Xen, Xen Cloud Platform ja XenServer. Se otettiinkin kiinteäksi osaksi Linuxia kernel version 3.3 julkaisun yhteydessä aiemman Linux bridge -reitittimen rinnalle. Tämän lisäksi se on käännetty lukuisille muille käyttöjärjestelmille, kuten FreeBSD ja Windows. Tämänhetkisen LTS-julkaisun versio on 1.9.x. (Mt.)

Open vSwitch ei itsessään ole hajautettu kytkin, mutta se mahdollistaa verkon keskitetyn hallitsemisen tukemalla tällä hetkellä kahta avointa protokollaa verkon hallitsemiseksi keskitetyltä kontrollerilta. Nämä protokollat ovat luvussa 2.4.1 mainitut OpenFlow sekä OVSDB. (Mt.)

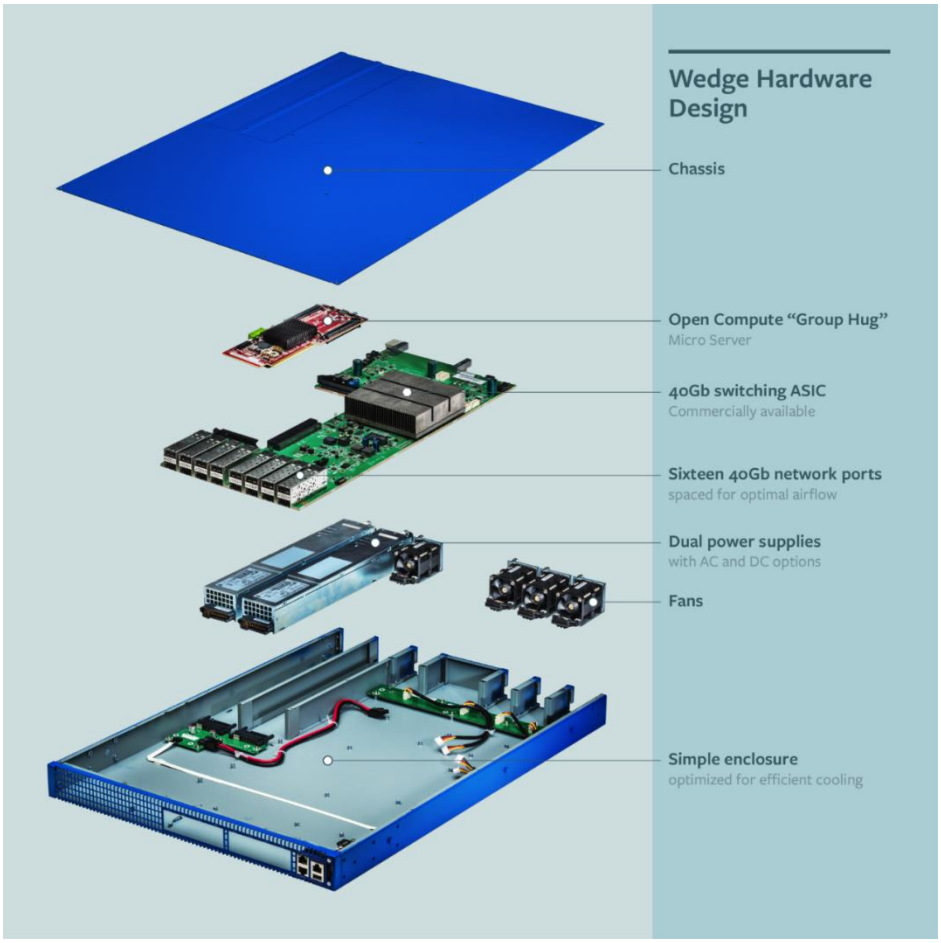
Open vSwitchin dokumentaatiossa kehotetaan varmistamaan liikenne OpenFlow-kontrollerille rakentamalla verkko OpenSSL:n kera. OpenSSL tukee vuonna 1999 julkaistua TSLv1-suojausta, jonka pitäisi olla yhteensopiva kaikkien modernien ohjelmistojen ja laitteiden kanssa. (Open vSwitch SSL 2014.)

6.2 Facebook Wedge ja Open Compute Project

Wedge on Facebookin kehittämä avoimeen lähdekoodiin perustuva kytkin. Kytkin sisältää Intelin mikropalvelimen, joka mahdollistaa sen toimimisen sekä kytkimenä että palvelimena. Laitteen mukana tulee Linuxiin perustuva FBOSS käyttöjärjestelmä. Se on suunniteltu helpottamaan verkkoinsinöörien työtä hallitsemalla laitteistoa ja seuraamalla sen suorituskykyä. Wedge myös hyödyntää Facebookin tammikuussa 2013 julkaisemaa Group Hug -mikropiiriä, jonka avulla FBOSS:ää voidaan ajaa millä tahansa suoritinpiirillä ja mahdollistaa sen käyttämisen muiden avointen tai kaupallisten verkkotuotteiden rinnalla. Kytkin tarjoaa 40 gigabittiä dataa sekunnissa, joka vastaa useita nykyisiä korkeamman tason kytkimiä. Lähitulevaisuudessa tämä on tarkoitus nostaa 10 gigatavuun sekunnissa. (Arce 2014.)

Kunhan sen testaus on valmis, Facebook Wedge tullaan julkaisemaan osana laajempaa Facebookin Open Compute Project -ohjelmaa, jonka alla julkaistaan avoimia räkki-, palvelin-, varastolaite-, ja muita tietotekniikkalaitesuunnitelmia. Laitteet julkaistaan hajotettuina, jolloin kaikki laitteiden ohjelmistojen ja raudan komponentit ovat vapaasti nähtävissä. Wedge ei ole tältä osin poikkeus. ja osaavissa käsissä myös muokattavissa tarpeen mukaisiksi niin laitteiston kuin ohjelmiston puolelta. Esimerkiksi porttien määrä on muokattavissa ja FBOSS Linuxin päälle voidaan rakentaa omia sovelluksia. (Miller 2014.)

Kuten kuviosta 14 näkee, koostuu Facebook Wedge ”group hug”-mikropalvelimesta, 40 Gb ASIC-lankusta, kuudestatoista 40 Gb portista, kahdesta virtalähteestä, tuulettimista sekä tehokkaasti viilennettävästä kotelosta. (Mt.)



Kuvio 14. Facebook Wedge osiin hajotettuna

Open Compute Project itsessään sai alkunsa, kun kolme Facebookin insinööriä Prinevillessä päättivät rakentaa kaikki datakeskuksen osat palvelimista aina räkkeihin ja virranjakeluun alusta alkaen itse. Lopputuloksena Prinevillen datakeskus kulutti 38 % vähemmän sähköä ja oli 24 % edullisempi rakentaa, kuin Facebookin aiemmat datakeskukset. Facebookin tavoite Open Compute Projectilla onkin herättää yhteistyötä ja parantaa nykyisiä suunnitelmia entistäkin tehokkaammiksi. (About Open Compute Project 2014.)

6.3 Muut valmistajat

SDN-tuki löytyy tavalla tai toisella käytännössä jokaisen valmistajan tuotteista. Sen sijaan täysi OpenFlow-tuki on tehnyt tuloaan laitteisiin vasta hiljalleen. Olen listannut tähän muutaman valmistajan, joiden laitteista OpenFlow-tuki nykyään löytyy.

Brocade

Brocade julkaisi omat OpenFlow-kytkimensä marraskuussa 2014, sekä päivitti OpenFlow 1.3 tuen kaikille vanhoille ICX-sarjan kytkimille (Brocade OpenFlow 2014).

HP

HP julkaisi kytkimiinsä vapaasti ilman erityistä lisenssiä ladattava OpenFlow-yhteensopiva ohjelmiston joulukuussa 2011. (HP OpenFlow Firmware 2011).

Juniper

Juniper on julkaissut OpenFlow-tuen lukuisille Junos OS -käyttöjärjestelmällä varustetuille laitteille. Näihin kuuluvat EX4550, EX9200 ja QFX5100 -kytkimet, sekä MX80, MX240, MX480 ja MX960 -reitittimet. Näistä kaikki paitsi EX4550 tukevat OpenFlow versiota 1.3.1. (Junos OS OpenFlow Support 2014.)

7 Muita SDN-projekteja

7.1 Yleistä SDN-projekteista

Koska SDN on tällä hetkellä tietoverkkojen puhutuimpia ja kuumimpia aiheita, eikä siitä huolimatta ole käytössä valtaosassa organisaatioita tai verkkoja millään tapaa, muodostaa se varsin uniikin markkinaraon. Käytännössä jokainen voi siitä hyötyä, joten lukuiset projektit mainostavat joko SDN-yhteensopivuutta, OpenFlow-tukea, tai muuten kehittävät sitä sivuavia tuotteita.

Käytännössä kaikki ratkaisut käyttävät OpenFlow-protokollaa, joka olikin alkujaan lähes synonyymi SDN:n kanssa. Tähän osioon olen listannut tunnettuja OpenFlown joko käyttöön ottaneita tai sen hyödyntämiä projekteja.

7.2 XenServer

XenServer on Citrixin hallinnoima avoimen lähdekoodin projekti ja yhteisö. Projekti kehittää avoimen lähdekoodin ohjelmistoa turvalliseen usean käyttöjärjestelmän ja sovelluksen pyörittämiseen yhdellä laitteella, mahdollistaen fyysisten laitteiden määrän tiivistämisen (eng: hardware consolidation) ja automatisoinnin tavoitteenaan leikata kuluja ja yksinkertaistaa palvelinten ja ohjelmien hallintaa. Citrix tarjoaa myös kaupallista tukea ja palveluita XenServerille suuryritysluokan lisenssisopimuksella sitä tarvitseville. (About XenServer 2014.)

Xen sai alkunsa Cambridgen yliopiston tutkimusprojektina vuonna 2003. Tulevina vuosina Xen hypervisorin ottivat käyttöön mm. Red Hat, Novell ja Sun. Lokakuussa 2007 Xen Project siirtyi Citrixin omistukseen. Vuoden 2013 huhtikuussa Xen Project siirrettiin Linux Foundationin alle yhteisprojektiksi. Linux Foundation otti sen Xen Project tavaramerille ja aloitti sille oman verkkosivunsa xenproject.org. Projektissa olivat mukana Citrixin lisäksi Amazon, AMD, Bromium, CA Technologies, Calxeda,

Cisco, Citrix, Google, Intel, Oracle, Samsung ja Verizon. Kaksi kuukautta myöhemmin Citrix julkisti myös avoimen lähdekoodin XenServer projektin, tarkoituksenaan tarjota heidän aiemmin suljettua tuotetta avoimesti avoimen lähdekoodin yhteisön vaikutettavaksi. (Mt.)

OpenFlown kannalta XenServerin tekee merkittäväksi se, että se oli ensimmäinen hypervisor-alusta OpenFlow tuella, jonka se sai jo joulukuussa 2010 Open vSwitchin avulla (Stocker 2011). Vuoden 2011 syyskuussa julkaistussa 6.0 versiossa Open vSwitch ja OpenFlow olivat oletuksena käytettävissä kaikissa asennuksissa. (Carovano 2011.)

7.3 OpenStack

OpenStack on avoimen lähdekoodin ilmainen alusta pilvipalveluille. Se on perustettu Rackspace Hostingin ja NASA:n yhteistyössä heinäkuussa 2010. Projekti sai oman kattojärjestönsä nimeltää OpenStack Foundation syyskussa 2012, jolloin OpenStack-yhteisöön kuului 550 jäsentä kaikkiaan 180 yrityksestä. (OpenStack Launches 2012). Viimeisenä kahtena vuonna OpenStack Foundation on kasvanut huomattavasti ja nykyään siihen kuuluu 9 500 jäsentä 850 eri organisaatiosta (OpenStack Foundation 2014).

OpenStack on perinteisten pilvipalveluiden lisäksi käytössä lukuisissa eri järjestelmissä, aina käyttöjärjestelmistä, maksupalveluiden tarjoajiin, verkkolaitevalmistajiin ja koulutuslaitoksiin. Sen käyttäjiin kuuluu muun muassa Dell, HP, IBM, Intel, VMware, Cisco, PayPal, Opera, Red Hat, AT&T, Orange, Sony Network Entertainment ja Disney. (OpenStack Companies 2014.)

OpenStack perustuu vahvasti modulaarisuuteen. Sen verkkorajapinnoista vastaa nykyään Neutron, joka on kehitetty ohjelmoitavaksi verkkopalveluksi, jolla asiakkaat voivat luoda omia verkkojaan.

8 Pohdinta

8.1. Tavoitteet, tulokset ja ongelmat

Opinnäytetyön aihe oli ”SDN:n tutkimustilanteen nykytilan kartoitus kyberturvallisuuden viitekehyksessä”. Tavoitteeksi olin kirjannut tutustuminen SDN-verkkojen nykytilaan, mukaan lukien tämänhetkiset laitteet, protokollat ja valmiit ratkaisut. Erityishuomiona oli katsastaa tietoturvan tila ja verrattiin siltä osin perinteisempiin verkkoratkaisuihin.

En tiedä kuinka paljon lopulta työhön tuli tutkimustilanteesta tai kyberturvallisuudesta, mutta nykytila kävi selväksi, samoin kuin monilta osin myös alan ammattilaisten tietämättömyys siitä mitä SDN verkon tietoturvalle tarkoittaa. Sen verran on selvää, että SDN kehittyy niin avoimissa projekteissa kuin suljettujen ovien takana. Pelkästään tämän kolmen kuukauden aikana on muun muassa avattu HP SDN App Store sekä julkaistu HP-VMware-ratkaisu. Lisäksi Facebook avasi uutta palvelinkeskustaan ja sen toimintaa, sekä kokonainen uusi käyttöjärjestelmä verkon runko-operaattoreiden käyttöön julkaistiin.

Aiheesta ei tullut vastaan käytännössä mitään suomenkielistä materiaalia, tai se on itselle tuntemattomammalta ohjelmoinnin puolelta, joten iso osa termeistä on joko sellaisenaan laitettuja tai vaan suoraan käännettyjä. Ajasta ja turhautumisesta iso osa johtui juurikin kielestä ja käännösongelmista, mikä vei aikaa ja energiaa itse työn tekemisestä. Aiheesta pitäisikin saada joko kattava sanakirja tai jokin suomalainen asian kattava teos.

8.2 SDN Buzzwordinä

SDN, tai Ohjelmallisesti määritetty verkko, on selvästi iso asia jo nyt ja mahdollisesti entistä suurempi tulevina vuosina. Termin ympärillä pyörinyt keskustelu, sadoista

miljoonista yli miljardiin dollariin pyörineet yrityskaupat, sekä Googlen ja Facebookin SDN-pohjaiset runkoverkkoratkaisut todistavat, että kiinnostusta alalla selvästi löytyy. Valitettavasti kiinnostuksen myötä samaan aikaan on kasvanut myös itse termin totaalinen muuntuminen ns. ”marchitectureksi”, joka tulee englannin kielen sanoista markkinointi ja arkkitehtuuri. Myöskin ainoana oikeana SDN-protokollana pidetyn OpenFlown ympärille alkoi hiljalleen ilmestyä kilpailevia ratkaisuja täysin uusista protokollista (OpFlex) vanhojen protokollien uusiokäyttöön (BGP, XMPP). Jotkut valmistajat ovat jopa markkinoineet NETCONF-yhteensopivia laitteitaan SDN-tuotteina.

SDN ei ole selvästikään menossa mihinkään terminä, mutta sen tarkka tarkoitus on selvästi kadonnut. Nykyään yhtä mieltä ollaan lähinnä siitä, että SDN-ratkaisussa verkkoylläpitäjän pitää voida syöttää kaikki komennot yhteen ohjelmistoon, joka ne älykkäästi jakaa eteenpäin verkon laitteille.

8.3 Kontrolleriviidakko

Tarkoituksenani oli alkujaan katsoa läpi kaikki SDN-kontrollerit, mutta hyvin pian kävi selväksi, että verkossa julkisesti saatavissa oleva tieto oli vahvasti markkinointihenkistä, tai muuten rajattua. Vertailu olisikin pitänyt tehdä ilmaiseksi saatavilla olevien kontrollerien välillä esimerkiksi mininet-verkkoa hyödyntäen. Tämä olisi käytännössä edellyttänyt kokonaisen testiympäristön pystyttämisen ja opiskelun, eikä ollut opinnäytetyön aikataulun rajoissa mahdollista.

Sen verran kontrollereista selvisi, että tulevaisuudessa OpenDaylightilla tulee olemaan yhteisönsä ansiosta vahva asema SDN-markkinoilla. Myös Project Floodlight on selvästi esillä ja onkin jo käytössä Big Switch Networksin kaupallisissa SDN-ratkaisuissa, sekä helposti saatavilla testikäyttöön pienempiin testi- ja opiskelutarkoituksiin.

Kaupallisista ratkaisuista HP:llä oli kokonaisvaltainen paketti myynnissä ja hinnoiteltuna. VMwarella tuntuu olevan tekniikka kasassa ja HP hyödyntääkin osittain VMwaren tekniikkaa oman ratkaisunsa toteutuksessa. Myös Juniper oli pistänyt lusikkansa moneen soppaan heidän Contrail-ratkaisulla ja sen turvallisempana vaihtoehtona mainostetulla hybridi-SDN:llä.

Kaikkein epäselvimpiä olivat Ciscon SDN-ratkaisut. Cisco on uudelleenpaketoinut ja uudelleennimennyt ratkaisujaan vuodesta toiseen, jättäen jälkeensä kunnollisen lyhennerykelmän: ONE, ACI, onePK, oneDK, ESP, EPN, APIC… Tietysti koska jokaiselle ratkaisulle on luvattu pitkää tukea tulevaisuuteen, löytyy Ciscolta verkkosivuiltaan paljon päällekkäistä ja sekavaa tietoa. Kaikesta käy ilmi Ciscon tarve pitää kiinni vanhasta markkina-asemastaan uusien ja vanhojen yrittäjien keskellä nopeasti muuttuvilla markkinoilla.

Kaiken kaikkiaan SDN on sellaisenaan erittäin epäselvä mutta tärkeä osa tietoverkkoja, ja tulee tulevaisuudessa vaikuttamaan suuresti alan työllisyysnäkymiin keskittämällä entistä enemmän töitä tietoverkkojen hallinnasta pilven ylläpitoon ja verkon sovellusten kehittämiseen.

Lähteet

About Open Compute Project 2014. Verkkosivut. Viitattu 1.11.2014. http://www.opencompute.org/about/

About XenServer 2014. Verkkosivut. Viitattu 27.10.2014. http://www.xenserver.org/about-xenserver-open-source.html

Arce, N. 2014. Facebook unveils open-source networking switch. Sucker punches Cisco?. Viitattu 30.10.2014. http://www.techtimes.com/articles/8791/20140620/facebook-unwraps-open-source-networking-switch-sucker-punches-cisco.htm

Banks E. 2014. SDN showdown: Examining the differences between VMware's NSX and Cisco's ACI. Viitattu 6.12.2014. http://www.networkworld.com/article/2172922/sdn/sdn-showdown--examining-the-differences-between-vmware-s-nsx-and-cisco-s-aci.html

Big Data Blog 2014. 7 Advantages of Software Defined Networking. Viitattu 3.12.2014. http://www.im-techsolutions.com/big-data/7-advantages-of-software-defined-networking

Big Network Controller 2014. Verkkosivu. Viitattu 7.12.2014. http://bigswitch.com/products/SDN-Controller

Bort, J. 2013. Here's What Happened When Cisco Lost A $1 Billion Deal With Amazon. Viitattu 5.11.2014. http://www.businessinsider.com/source-cisco-1b-amazon-deal-led-to-insieme-sdn-2013-10

Brant, P. 2013. The Software-Defined Data Center: The Three Caballeros Finally Have Their Cloudy Day. Software-Defined Networking (SDN). Books24x7.

Brocade OpenFlow 2014. Brocade Advances SDN Leadership With OpenFlow 1.3 Support Across IP Routing and Switching Portfolio. Viitattu 7.12.2014. http://newsroom.brocade.com/press-releases/brocade-advances-sdn-leadership-with-openflow-1-3--nasdaq-brcd-1094247

Carovano, B. 2011. XenServer 6.0 is here!. Viitattu 27.10.2014. http://blogs.citrix.com/2011/09/30/xenserver-6-0-is-here/

Cisco ACI Security 2014. A New Approach to Secure the Next - Generation Data Center. Viitattu 7.11.2014. http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-732354.pdf

Cisco onePK 2014. One Platform Kit (onePK) for Developers. Viitattu 20.10.2014. http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/at_a_glance_c45-708540.pdf

Cisco OpFlex 2014. OpFlex: An Open Source Approach. Viitattu 26.10.2014. http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731304.pdf

Contrail Networking 2014. Contrail Networking. Data Sheet. Viitattu 7.12.2014.

http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000521-en.pdf

Data Centers Ill-Equipped 2013. Global Study Finds Data Centers Ill-Equipped to Serve Demands in the Era of Virtualization and Cloud. Viitattu 14.11.2014. http://newsroom.brocade.com/press-releases/global-study-finds-data-centers-ill-equipped-to-se-nasdaq-brcd-1032499

Dix, J. 2012. Google's software-defined/OpenFlow backbone drives WAN links to 100% utilization. Viitattu 2.1.2014. http://www.networkworld.com/article/2189197/lan-wan/google-s-software-defined-openflow-backbone-drives-wan-links-to-100--utilization.html

Duffy, J. 2013. Skepticism follows Cisco-IBM led OpenDaylight SDN consortium. Viitattu 9.11.2014. http://www.networkworld.com/article/2165155/lan-wan/skepticism-follows-cisco-ibm-led-opendaylight-sdn-consortium.html

Duffy, J. 2014. Cisco reveals OpenFlow SDN killer. Viitattu 7.11.2014. http://www.networkworld.com/article/2175716/lan-wan/cisco-reveals-openflow-sdn-killer.html

Dutt, D. 2013. Your next network operating system is Linux. Viitattu 22.10.2014. http://www.infoworld.com/article/2612738/networking/your-next-network-operating-system-is-linux.html

Floodlight 2014. Verkkosivu. Viitattu 18.11.2014. http://www.projectfloodlight.org/floodlight/

Floodlight Getting Started 2014. Verkkosivu. Viitattu 7.12.2014. http://www.projectfloodlight.org/getting-started/

Floodlight Indigo 2014. Verkkosivu. Viitattu 18.11.2014. http://www.projectfloodlight.org/indigo/

Google WAN 2012. Google Inter-Datacenter WAN with centralized TE using SDN and OpenFlow. Viitattu 1.12.2014. https://www.opennetworking.org/images/stories/downloads/sdn-resources/customer-case-studies/cs-googlesdn.pdf

Google 10G switch 2007. Google’s Secret 10GbE Switch. Viitattu 5.11.2014. http://www.nyquistcapital.com/2007/11/16/googles-secret-10gbe-switch/

Hedlund, B. 2013. What is a Distributed Firewall? Viitattu 6.12.2014. http://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html

Hoezle, U. 2012. OpenFlow @ Google. Viitattu 1.12.2014. http://www.opennetsummit.org/archives/apr12/hoelzle-tue-openflow.pdf

HP OpenFlow Firmware 2011. HP OpenFlow capable firmware is now GA. OpenFlow Blog. Viitattu 23.11.2014. http://archive.openflow.org/wp/2011/12/hp-openflow-capable-firmware-is-now-ga/

HP SDN App Store 2014. HP Launches Industry’s First SDN App Store, Unleashing New Wave of Networking Innovations. Viitattu 23.11.2014. http://www8.hp.com/us/en/hp-news/press-release.html?id=1798074

HP SDN NV 2014. Software-defined networking and network virtualization. Technical white paper. Viitattu 23.11.2014. http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA5-0092ENW.pdf

HP VAN SDN 2014. HP VAN SDN Controller Software. Data sheet. Viitattu 23.11.2014. http://h20195.www2.hp.com/v2/getpdf.aspx/4AA4-9827ENW.pdf

HP-VMware 2014. Greater agility and continuity Brochure. Viitattu 23.11.2014. http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4307ENW&cc=us&lc=en

Johnson, S. 2013a. Border Gateway Protocol as a hybrid SDN protocol. Viitattu 1.12.2014. http://searchsdn.techtarget.com/feature/Border-Gateway-Protocol-as-a-hybrid-SDN-protocol

Johnson, S. 2013b. The role for XMPP as a southbound SDN protocol. Viitattu 1.12.2014. http://searchsdn.techtarget.com/feature/The-role-for-XMPP-as-a-south-bound-SDN-protocol

Junos OS OpenFlow Support 2014. OpenFlow Support on Devices Running Junos OS. Viitattu 7.12.2014. http://www.juniper.net/documentation/en_US/release-indepen-dent/junos/topics/reference/general/junos-sdn-openflow-supported-platforms.html

JYVSECTEC 2014. Verkkosivu. viitattu 14.11.2014. http://jyvsectec.fi/jyvsectec/

Lawson, S. 2013. Network heavy hitters to pool SDN efforts in OpenDaylight project. Viitattu 9.11.2014. http://www.networkworld.com/article/2165112/smb/network-heavy-hitters-to-pool-sdn-efforts-in-opendaylight-project.html

Malik, O. 2012. Cisco memo: We can't build anything. Viitattu 5.11.2014. https://gigaom.com/2012/04/19/cisco-memo-we-cant-build-anything/

Matsumoto, C. 2014. Cisco Slims Its SDN Story Down to ONE Controller. Viitattu 6.11.2014. https://www.sdncentral.com/news/cisco-slims-sdn-story-one-controller/2014/03/

McGillicuddy, S. 2014. An in-depth look at the network in the Facebook Altoona data center. Viitattu 1.12.2014. http://searchsdn.techtarget.com/news/2240235446/An-in-depth-look-at-the-network-in-the-Facebook-Altoona-data-center

Miller, R. 2014. Facebook's New Open-Source Data Switch Technology Is Designed For Flexibility And Greater Control. Viitattu 30.10.2014. http://techcrunch.com/2014/06/18/facebooks-new-open-source-data-switch-technology-is-designed-for-flexibility-and-greater-control/

Möller, B., Duong T. & Kotowicz K. 2014. This POODLE Bites: Exploiting The SSL 3.0 Fallback. Viitattu 26.10.2014. https://www.openssl.org/~bodo/ssl-poodle.pdf

ONF Formed 2011. Open Networking Foundation Formed to Speed Network Innovatio. OpenFlow Blog. Viitattu 4.9.2014. http://archive.openflow.org/wp/2011/03/open-networking-foundation-formed-to-speed-network-innovation/

ONF SDN New Norm 2012. Software-Defined Networking: The New Norm for Networks. ONF White Paper. Viitattu 22.11.2014. https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

ONF SDN Security Considerations 2013. SDN Security Considerations in the Data Center. ONF Solution Brief. Viitattu 15.10.2014. https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf

Open vSwitch FAQ 2014. Frequently Asked Questions. Viitattu 12.10.2014. https://github.com/openvswitch/ovs/blob/master/FAQ.md

Open vSwitch SSL 2014. Configuring Open vSwitch for SSL. Viitattu 22.10.2014. http://git.openvswitch.org/cgi-bin/gitweb.cgi?p=openvswitch;a=blob_plain;f=INSTALL.SSL;hb=HEAD

OpenContrail FAQ 2014. Verkkosivu. Viitattu 7.12.2014. http://www.opencontrail.org/frequently-asked-questions-faq/

OpenFlow Enabling Innovation 2008. OpenFlow: Enabling Innovation in Campus Networks. OpenFlow White Paper. Viitattu 15.10.2014, http://archive.openflow.org/documents/openflow-wp-latest.pdf

OpenFlow MythBusting 2012. OpenFlow MythBusting by Google. Viitattu 29.11.2014. http://www.bigswitch.com/blog/2012/04/30/openflow-mythbusting-by-google

OpenStack Companies 2014. Verkkosivu. Viitattu 6.10.2014. http://www.openstack.org/foundation/companies/

OpenStack Foundation 2014. Verkkosivu. Viitattu 6.10.2014. http://www.openstack.org/foundation/

OpenStack Launches 2012. OpenStack Launches as Independent Foundation, Begins Work Protecting, Empowering and Promoting OpenStack. Viitattu 6.10.2014. http://www.businesswire.com/news/home/20120919005997/en/OpenStack-Launches-Independent-Foundation-Begins-Work-Protecting

Pfaff, B., Davie B. 2013. The Open vSwitch Database Management Protocol. Viitattu 19.11.2014. https://tools.ietf.org/html/rfc7047

POODLE FALLBACK 2014. POODLE and the TLS_FALLBACK_SCSV Remedy. Viitattu 26.10.2014. http://www.exploresecurity.com/poodle-and-the-tls_fallback_scsv-remedy/

Prince, M. 2014. SSLv3 Support Disabled By Default Due to POODLE Vulnerability. Viitattu 21.10.2014. http://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/

Kerner, S. M. 2013. Juniper Builds SDN Controller with XMPP. Viitattu 4.12.2014. http://www.enterprisenetworkingplanet.com/datacenter/juniper-builds-sdn-controller-with-xmpp.html

SDN App Store 2014. Verkkosivu. Viitattu 6.12.2014. https://hpn.hpwsportal.com/catalog.html#/Home/Show

Sowell, G. 2013. OpenFlow And Mikrotik. Viitattu 4.12.2014. http://gregsowell.com/?p=4442

Stocker J. 2011. How OpenFlow is changing networking and XenServer. Viitattu 27.10.2014. http://blogs.citrix.com/2011/05/16/how-openflow-is-changing-networking-and-xenserver/

Technical Overview 2014. Verkkosivu. Viitattu 11.11.2014. http://www.opendaylight.org/project/technical-overview

Tutustu JAMKiin 2014. Verkkosivu. Viitattu 14.11.2014. http://www.jamk.fi/fi/Tietoa-JAMKista/Tutustu-JAMKiin/

What is OVSDB? 2014. What is OVSDB?. Viitattu 20.11.2014. https://www.sdncentral.com/resources/open-source/what-is-ovsdb/

VMware NSX 2013. The VMware NSX Network Virtualization Platform. Technical White Paper. Viitattu 2.11.2014. http://www.vmware.com/files/pdf/products/nsx/VMware-NSX-Network-Virtualization-Platform-WP.pdf